Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет информационной безопасности

Кафедра защиты информации

Т. В. Борботько, О. В. Бойправ, А. М. Тимофеев

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Допущено Министерством образования Республики Беларусь
в качестве учебного пособия
для студентов учреждений высшего образования по профилю образования
«Информационные и коммуникационные технологии», по группе
специальностей «Электроника и автоматизация»
и по специальностям «Нанотехнологии и наноматериалы»,
«Инженерно-педагогическая деятельность»*

Минск БГУИР 2025

УДК 004.56(076)
ББК 32.972.5я73
Б82

Р е ц е н з е н т ы:

кафедра математического моделирования и анализа данных
факультета прикладной математики и информатики
Белорусского государственного университета
(протокол № 1 от 29.08.2024);

заведующий лабораторией проблем защиты информации
ГНУ«Объединенный институт проблем информатики
Национальной академии наук Беларуси»
кандидат физико-математических наук В. А. Дмитриев

Борботько, Т. В.

Б82 Основы информационной безопасности : учеб. пособие / Т. В. Борботько, О. В. Бойправ, А. М. Тимофеев. – Минск : БГУИР, 2025. – 128 с. : ил.
ISBN 978-985-543-826-8.

Содержит теоретические материалы по дисциплине «Основы информационной безопасности».

УДК 004.56(076)
ББК 32.972.5я73

ISBN 978-985-543-826-8

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 4
1. ЖИЗНЕННЫЙ ЦИКЛ ИНФОРМАЦИИ 5
2. ИНФОРМАЦИЯ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ
И ЕЕ ДЕМАСКИРУЮЩИЕ ПРИЗНАКИ 19
3. МОДЕЛЬ НАРУШИТЕЛЯ 36
4. СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
РЕСПУБЛИКИ БЕЛАРУСЬ 45
5. МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ 51
6. СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ 57
7. ФИЗИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ 68
8. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ 75
9. ЗАЩИТА ИНФОРМАЦИИ ОТ ТЕХНИЧЕСКОЙ РАЗВЕДКИ 88
10. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ 99
11. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ 111
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 126

ВВЕДЕНИЕ

Бизнес-процессы в организациях, ориентированных на производство товаров или предоставление услуг, позволяет им получать прибыль, которая по определенным правилам перераспределяется среди сотрудников организации, участников такой совместной последовательной деятельности. Появление прибыли в организации, а у ее сотрудников – заработной платы позволяет обеспечить ее устойчивое функционирование, кроме этого, часть прибыли идет не развитие, покупку нового оборудования, оплату коммунальных услуг, возвращение кредитных средств, взятых на развитие бизнеса.

Обеспечение вышеуказанной деятельности организаций реализуется посредством информационных систем, применение которых и позволяет обеспечить бизнес-процессы. В такого рода системах накапливаются, обрабатываются и хранятся сведения, которые позволяют организациям обеспечивать свои бизнес-процессы и извлекать из них прибыль. Поэтому критически важным для организации является обеспечение надежного хранения сведений, которыми они обладают, и обеспечение стабильности функционирования своих информационных систем.

Понимание, насколько эти два процесса являлись важными, к сожалению, наступает после того, когда организациям наносится ущерб, связанный с утечкой информации и невозможностью эксплуатации в нормальном режиме информационных систем. Информация сегодня – это деньги, и ее передача третьим лицам – это, по своей сути, передача им денежных средств. Конкурентная борьба на рынках строится на использовании эффективных стратегий, а для ее построения необходимы сведения. Исходя из чего, контроль доступа к информации, а по сути – к носителю, на котором она содержится, – это контроль доступа к денежным средствам. К сожалению, ценность утраченных сведений часто осознают после их утраты.

В учебном пособии рассматриваются вопросы, связанные с рядом мероприятий, которые необходимо реализовать, для того чтобы обеспечить контролируемый доступ к сведениям, носителями которых являются не только бумажные документы, но и информация в электронном виде (файлы), а также физические поля. Рассмотрены правовые, организационные и технические методы защиты информации, которая относится к охраняемой законом тайне. Отдельный раздел посвящен вопросам социальной инженерии, которая сегодня широко используется не только для получения нарушителем доступа к носителю информации, но и мошенниками при их доступе к финансовым средствам физических и юридических лиц.

1. ЖИЗНЕННЫЙ ЦИКЛ ИНФОРМАЦИИ

Основная терминология темы [1]. **База данных** – совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях.

Банк данных – организационно-техническая система, включающая одну или несколько баз данных и систему управления ими.

Вербальная коммуникация – взаимодействие людей, построенное с использованием ими лексически выделенных единиц (слов).

Дезинформация – ложные сведения, навязываемые одной стороной, участвующей в коммуникации, другой стороне с целью введения ее в заблуждение и в конечном итоге принятия неверного ею решения.

Защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств.

Информационная технология – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации.

Информационные отношения – отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий.

Информационное противоборство – целенаправленное и планомерное информационно-психологическое воздействие на человека, группу людей или общество за счет использования таких способов предоставления информации, которые позволяют в значительной степени активизировать переживания и тем самым изменить психическое состояние и снизить активность применения критического мышления в процессе восприятия предоставляемой информации.

Критическое мышление – способность человека, заключающаяся в проведении подробного анализа получаемой им информации за счет сопоставления анализируемых им сведений и накопленной ранее достоверной информации с целью выявления их несоответствия с последующим отвержением несоответствующих сведений.

Невербальная коммуникация – взаимодействие людей, построенное на использовании ими жестикуляции, мимики и т. д. в процессе вербальной коммуникации.

Носитель информации – материальный объект, на котором сведения содержатся в виде символов, образов, сигналов и (или) технических решений и процессов, позволяющих их распознать и идентифицировать.

Обладатель информации – субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства, или по договору.

Пользователь информации – субъект информационных отношений, получающий, распространяющий и (или) предоставляющий информацию, реализующий право на пользование ею.

Предоставление информации – действия, направленные на ознакомление с информацией определенного круга лиц.

Распространение информации – действия, направленные на ознакомление с информацией неопределенного круга лиц.

Значимость информации для человека. Информация необходима человеку для того, чтобы принять верное решение по тому или иному вопросу (сделать правильный выбор). Человек воспринимает информацию используя различные органы чувств, основными из которых являются зрение и слух. Любой человек – часть общества, и поэтому важным для него способом получения информации является коммуникация, в частности вербальная (передача сведений с помощью речи) и невербальная (использование жестов, мимики, интонации и т. д.). Как правило, вербальная и невербальная коммуникации неразрывно связаны друг с другом.

Преобладание невербальной коммуникации у человека может быть обусловлено тем, что он плохо владеет языком, на котором осуществляется вербальная коммуникация (недостаточность словарного запаса и (или) неспособность его правильно применять), а также эмоциональным состоянием человека.

Воспринимая информацию, человек аккумулирует ее в виде знаний, которые впоследствии могут быть использованы им для принятия решений. Многие люди хотели бы не ошибаться в жизни и принимать верные решения. Именно для этого им нужна достоверная (подлинная, не ложная) информация.

Для принятия решения необходимо обладать достоверной и полной (подробной) информацией. Так, например, отправляющемуся в поездку на поезде человеку необходимо знать не только дату и время отправления поезда, но и номер платформы и пути отправления.

Для того чтобы повлиять на принимаемое человеком решение, ему необходимо сообщить и внушить ложную информацию (дезинформацию).

Формирование, предоставление и навязывание дезинформации составляет суть информационного противоборства, что позволяет влиять на знания человека и на решение, которое он примет в целом, используя накопленные или полученные ранее им знания.

При восприятии информации человеком не последнюю роль играет его эмоциональное состояние (угнетенность, подъем, бодрость и т. д.). Поэтому для адекватного восприятия информации важным является наличие у человека критического мышления.

Исходя из чего, важным процессом при усвоении некоторой информации является оценка ее достоверности. Проверка достоверности информации требу-

ет некоторого времени и является многостадийным процессом, в основу которого положен анализ содержания проверяемых сведений.

Для оценки достоверности информации необходимо иметь непосредственно сведения, достоверность которых необходимо оценить, а также их исходные данные (например, автор, источник, где они опубликованы, дата публикации и т. д.). Учитывая то, что в создании информации непосредственное участие принимает человек, соответственно именно он является автором различных сообщений, публикаций и т. д. Поэтому важным является доверие к автору оцениваемой на достоверность информации.

Методика оценки достоверности информации. На *первом этапе* методики выполняется именно такая проверка. Понимая сущность и тематику оцениваемой информации, необходимо обратить внимание на то, какие ранее информационные сообщения были опубликованы этим автором. Например, журналист, профессионал своего дела, всегда специализируется на определенной тематике. В процессе составления различных публикаций он постепенно обогащает свои знания и опыт по направлению специализации. Поэтому в его сообщениях в меньшей степени могут присутствовать сведения в виде оценки. Для уменьшения субъективизма в изложении материала такие журналисты прибегают к взаимодействию с не одним, а несколькими экспертами. Это трудоемкий и длительный по времени процесс, но он позволяет изложить материал более полно. С другой стороны, человек, который заинтересован в получении быстрого эффекта от публикации, навязывая определенное мнение, может излагать исключительно свою точку зрения или привлечь одного стороннего человека, обозначив его как эксперта по тематике сообщения. Такой подход минимизирует временные затраты при максимальном эффекте от подобным образом формируемого сообщения.

Поэтому важно проанализировать следующие сведения об авторе сообщения (информации).

1. Фамилия, имя, отчество, адрес электронной почты, его статус (журналист, главный редактор и т. д.) в рамках данного информационного ресурса, агентства и т. д., его положение в обществе.

2. Какова репутация автора, на чем он специализируется, является ли он экспертом по сути сообщения (сколько у него сообщений на подобную тему и каково их содержание (подробность изложения материала)). Если после прочтения сообщения возникают вопросы и есть недосказанность, то всецело доверять автору сложно.

3. Ссылается ли он в сообщении на какие-либо источники и можно ли этим источникам доверять.

На *втором этапе* выполняется анализ сведений об источнике информации (это может быть некоторое издание или электронный ресурс). Результатом данного этапа должно быть решение о том, можно ли доверять данному источнику информации.

Источники информации могут быть разнообразные: это средства массовой информации, которые аккредитованы в Республике Беларусь; различные

электронные ресурсы; информация, предоставляемая блогерами и поступающая через различные социальные медиа (сети), телеграмм-каналы и т. д.

Гипотетически чем больше ссылок на источник информации можно найти, тем выше доверие к источнику и транслируемой с его помощью информации. Вместе с тем необходимо помнить о том, что современные информационно-коммуникационные технологии позволяют достаточно быстро наращивать количество просмотров и организовать множество ссылок на источник информации для того, чтобы создать иллюзию источника информации, которому можно доверять.

Репутация источника информации как достоверного формируется на протяжении длительного времени, поэтому необходимо иметь представление о том, какое время существует этот источник. Нужно помнить, что большое количество подписчиков не может являться критерием доверия к источнику информации. Следует внимательно относиться к источникам-«однодневкам», которые могут быть использованы для распространения дезинформации или недостоверной информации, т. е. информации, не являющейся фактами.

Источниками фактов могут быть: аккредитованные в Республике Беларусь средства массовой информации (предоставление такими источниками дезинформации приводит к отзыву лицензии и наступлению ответственности в соответствии с действующим законодательством), Национальный статистический комитет Республики Беларусь, научно-исследовательские институты и т. п.

Если средство массовой информации предоставляет какие-либо сведения без ссылки на их источник, то отнесение этих сведений к фактам является некорректным. Рассмотрим, например, сведения следующего содержания: «Ученые установили, что для похудения необходимо каждое утро выпивать стакан молока». Эти сведения сложно отнести к достоверной информации (т. е. к факту), так как в них представлена отсылка к такому «источнику», как «ученые», без указания конкретных фамилий.

Необходимо внимательно относиться к источникам информации, которые позиционируют себя как независимые средства массовой информации. Средству массовой информации нет необходимости заявлять или постоянно подчеркивать такой факт. Наличие подобных заявлений может быть типичной манипуляцией для привлечения внимания и навязывания дезинформации. Нужно помнить, что любой информационный ресурс требует определенных затрат от того юридического (организация) или физического (человек) лица, которое его поддерживает. Эти затраты в первую очередь финансовые (оплата электроэнергии, заработная плата, оплата хостинга и т. д.). Поэтому любой из источников информации будет определенным способом финансироваться или в противном случае спустя некоторое время прекратит свое существование, так как энтузиазм заканчивается ввиду снижения мотивации у человека с истечением времени.

На *третьем этапе*, прочитав и проанализировав сведения (например, публикацию в средствах массовой информации), необходимо вынести решение об отнесении содержания публикации к факту или оценке.

К фактам относят:

1) свершившиеся события (дата рождения, дата окончания школы, дата зачисления в университет и др.), т. е. имеющие некоторое численное измерение, что позволяет их проверить;

2) результат деятельности человека (построенный дом, спроектированное некоторое устройство и т. д.), который можно определенным образом осязать и измеряем в некотором численном эквиваленте (количество штук, геометрические размеры и т. д.).

К фактам относится все то, что поддается проверке (например, с помощью поисковых систем), измерению (например, с помощью измерительных средств), подтверждению (например, с помощью каталогов и материалов архивов), осязанию (результат можно потрогать руками).

Оценка, в свою очередь, является субъективной точкой зрения даже тогда, когда отражает взгляд целой группы людей (информация может быть им навязана) или человека, которого считают или называют экспертом. Оценка может даваться на основании:

– эмоционального восприятия человеком окружающего мира (происходящих событий);

– личных предпочтений человека;

– определенных жизненных позиций и устоев человека;

– приобретенного ранее опыта и накопленных знаний.

Известная фраза древнегреческого философа Сократа гласит: «В споре рождается истина».

Оценка часто содержит эмоциональную составляющую, которая побуждает человека к действиям, мотивирует его выполнить что-либо, изменить свое мнение – это один из важнейших признаков. Для его обнаружения необходимо внимательно прочитать анализируемую информацию и постараться обнаружить фразы или предложения, которые позволяют влиять на эмоциональное состояние человека.

Важным является подтверждение фактов несколькими источниками информации, что позволяет проверить анализируемые сведения на достоверность.

На заключительном, *четвертом этапе*, выполняется анализ полноты информации. Недосказанность порождает ряд вопросов и если они возникают, то тогда вполне вероятно, что признать информацию полной будет сложно. Вместе с тем при таком положении дел вполне вероятно, что не все сообщение, а какую-то его часть можно признать полной. Предположим, у нас есть инструкция по пользованию, например, смартфоном, из которой удалили некоторые страницы. Оставшаяся в ней информация является достоверной, но не полной, так как она не позволит в полной мере обеспечить использование такого устройства. Именно поэтому, оценивая достоверность сведений, важно иметь представление об их полноте.

По итогу анализа оцениваемой информации может сложиться такая ситуация, что она не в полном объеме, а некоторая ее часть будет достоверной,

именно эту часть сведений можно использовать в виде знаний и для дальнейшего принятия решения.

Требования к информации. Информация используется человеком для принятия решения, поэтому к ней предъявляются следующие требования, которые позволяют оценить ее качество.

1. Достоверность. Необходимо обладать точной информацией, неискаженной, это позволит принять правильное решение. В условиях обилия дезинформации следует оценивать достоверность сведений, что позволит минимизировать восприятие ложной (недостоверной) информации.

2. Полнота. Недостаток сведений приводит также к неверно принятым человеком решениям. Поэтому информация должна быть не только достоверной, но и полной. Для получения сведений в полном объеме человек обладает различными способами восприятия информации. На эти способы будет указано ниже.

3. Своевременность. Одна из важнейших характеристик информации. Достоверные и полные сведения нужны именно к тому моменту, когда человеку необходимо сделать выбор (принять решение). Наличие таких сведений после того, как будет принято решение, не способствует правильному выбору, а лишь позволяет оценить его верность постфактум.

Необходимо заметить, что важным в процессе принятия решения является восприятие информации человеком. Понимание того, каким образом человек воспринимает информацию, дает возможность эффективно доносить ее до него. Выделяют следующие способы восприятия информации человеком.

1. Визуальный. Восприятие информации реализуется посредством органов зрения. Этот способ является основным. Именно он позволяет человеку получать сведения об окружающем мире, и поэтому когда человек теряет зрение, то это существенно сказывается на его дальнейшей жизни. Люди так часто и говорят: «Пока не увижу – не поверю». Сегодня это часто используется для навязывания ложных сведений человеку в рамках информационного противоборства между странами. Поток сведений в виде изображений, видеороликов транслируется и выдается за достоверную информацию, при этом применяется технология нейронных сетей, которые позволяют такие изображения и видеоролики сделать максимально правдоподобными (deep fakes).

Поскольку визуальный способ является основным у человека для получения сведений, это необходимо учитывать при организации образовательного процесса или эффективной передаче информации человеку. Под эффективностью в данном случае подразумевается снижение временных затрат на процесс трансляции сведений человеку при том же объеме передаваемых сведений без потери «качества» усвоения транслируемой информации.

2. Аудиальный. Является вторым по значимости для человека способом восприятия информации. В данном случае для восприятия информации человек использует органы слуха. Речевая информация прекрасно дополняет транслируемые в виде графических образов сведения, воспринимаемые с помощью органов зрения, и позволяет дополнить их таким образом, чтобы человек их вос-

принял именно так, как это необходимо тому лицу, которое их передает. Например, в образовательном процессе преподаватель демонстрирует на лекции подготовленную им презентацию и поясняет (дополняет с помощью устной речи) ее. Низкоэффективным способом передачи информации будет тот случай, когда преподаватель начнет читать то, что написано на слайдах. При таком развитии ситуации дополнение сведений, воспринимаемых человеком с помощью органов зрения, не происходит, и предоставляемый таким образом материал будет восприниматься человеком так, как он понял исходя из тех знаний, которыми он обладает, и из того жизненного опыта, что он уже получил. Таким образом, в данном случае речь идет о дополнении сведений, которые человек получает с помощью органов зрения, теми сведениями, которые он получает с помощью органов слуха. Потеря слуха для человека является существенной проблемой, но не такой критичной, как потеря зрения, что подтверждается следующим высказыванием: «Береги как зеницу ока».

3. Другие способы восприятия информации. Сюда относят получение информации с помощь органов обоняния, осязания и вкуса. Сведения, полученные с помощью таких органов, дополняют информацию, полученную визуально и аудиально и позволяют обеспечить формирование целостной (полной) картины о том или ином объекте.

Рассмотрим пример, который объединяет все указанные способы восприятия информации при принятии решения человеком. Человек пришел на рынок, и ему необходимо купить яблоки. Товар ему нужен, бесспорно, самый лучший, но продавцов такого товара немало и вопрос выбора становится непростым. На первом этапе поиск и сравнение товара ведется с помощью органов зрения. Товар у разных продавцов сравнивается по внешнему виду и, конечно, по цене, так как яблоки нужны не только самого лучшего качества, но еще и недорогие (а еще внимание обращают на продавцов и не только на них). На втором этапе для уточнения характеристик товара покупатель вступает в речевую коммуникацию с продавцами и аудиально получает сведения, которые также использует для выбора товара. На третьем этапе задействуются органы осязания, обоняния и вкуса: яблоки с позволения продавца пробуют, трогают и подносят к носу, чтобы почувствовать запах. Применение такого многообразия способов восприятия информации позволяет получить достоверные полные сведения и сделать выбор. О правильности выбора судят обычно постфактум. Это объясняется тем, что восприятие информации эмоционально, а это, в свою очередь, влияет на критическое мышление (достоверность информации), и поэтому не исключается манипулирование со стороны продавца и навязывание ложной информации, а соответственно, продажа товара, который может не совсем подходить под требования покупателя.

Подводя итог, необходимо отметить, что принятие решения является абсолютно нетривиальной задачей. При передаче сведений от одного человека другому происходит обмен эмоциями, которые влияют на восприятие информации и в конечном итоге на поведение человека (на его действие или бездействие). Это широко используется сегодня при реализации информационно-

психологических операций, которые составляют основу информационного противоборства различных стран.

Создание информации. В этом процессе принимает участие человек, и он как автор или создатель информации имеет право ею распоряжаться, в том числе передавать право обладать ею другим людям.

Резюмируя вышеуказанное, следует отметить, что информация является предметом собственности и у нее есть обладатель. Обладателями информации являются:

1) физические лица – непосредственно люди;

2) юридические лица – организации, предприятия, фирмы и т. п.

3) Республика Беларусь.

Обладатель информации определяет, кому разрешить доступ к сведениям, которые он создал или получил на законных основаниях.

Виды информации. С учетом того, каким образом человек воспринимает информацию, ее можно разделить на виды.

Высказывание или текст представляют собой соответственно речевую информацию или информацию в виде символов на бумажных или электронных носителях, которую человек воспринимает соответственно с помощью органов слуха или зрения. С точки зрения передачи информации от человека к человеку, побуждения к действию или бездействию человека этот вид сведений является наиболее значимым для человека.

Изображение – сведения в виде рисунка или фотографии, которые человек воспринимает с помощью органов зрения.

Видеофильм – содержит в себе сведения, передаваемые в вербальной и/или невербальной форме и воспринимаемые органами зрения и слуха человека.

Все вышеуказанные виды информации могут иметь различные формы представления.

Формы представления информации. Выделяют следующие формы представления информации:

– **на бумажных носителях** – в виде текста или изображений;

– **на электронных носителях** – в виде текста, изображений или видеофильмов;

– **физические поля** (акустические или электромагнитные) – обеспечивают передачу информации в виде текста, изображений или видеофильмов.

Следует заметить, что посредством электромагнитного излучения радиочастотного диапазона длин волн представляется информация, предназначенная для передачи по беспроводным каналам связи, посредством электромагнитного излучения оптического диапазона длин волн (видимой и инфракрасной области спектра) представляется и передается информация о свойствах объектов, их месторасположении, состоянии.

Не следует путать понятия «представление информации» и «предОставление информации».

Под представлением информации понимается предъявление ее субъекту(-ам) информационных отношений для того, чтобы те могли с ней ознакомиться.

Очевидно, что такое действие не повлечет за собой последствий, связанных с изменением содержания информации.

Под предоставлением информации понимается передача информации в распоряжение субъектов информационных отношений. В таком случае можно ожидать того, что содержание информации может быть изменено субъектами, которым она была передана.

Носитель информации. На основании анализа форм представления информации можно сделать вывод о том, что носитель информации – это материальный объект. Получение человеком доступа к носителю информации дает ему возможность получить доступ к информации, которая на нем содержится. Материальным носителем являются, например, бумага или дисковые накопители (карты флеш-памяти, жесткие диски и т. п.).

Прием и передача информации. В процессе коммуникации человек передает и получает информацию, и эти процессы реализуются:

1) при физическом контакте людей – в данном случае сведения могут быть переданы на носителе, например, бумажном в виде текста, либо информация может быть передана устно, в виде речи;

2) посредством телекоммуникаций. Для этого используется комплекс технических средств, который обеспечивает передачу информации в определенной форме представления на расстояние, которое значительно превышает расстояние передачи речевой информации в устной или письменной формах от человека к человеку при их физическом контакте.

Передача сведений на значительные расстояния становится возможной благодаря их преобразованию в различные сигналы. Сигнал представляет собой физический процесс, который характеризуется некоторыми параметрами, например частотой, амплитудой, фазой, и он позволяет передавать информацию на определенные расстояния.

Выделяют следующие виды сигналов:

– акустический – способен распространяться в газообразной, твердой и жидкой средах в виде механических колебаний этих сред; на слух такой сигнал воспринимается человеком как звук;

– электрический – распространяется в материалах, проводящих электрический ток (проводниках), а также в газообразной (воздух) и твердой средах (ограждающие конструкции помещения – стены, потолок, пол) в форме электромагнитной волны; такой сигнал используется в электросвязи и радиосвязи для передачи информации на значительные расстояния посредством телекоммуникаций;

– **оптический** – распространяется в газообразной (воздух) и твердой (оптически прозрачных) средах, а также космическом пространстве; в качестве твердой среды в телекоммуникациях используют волоконно-оптические линии связи.

Преобразование информации. Исходя из того что телекоммуникации используются для передачи информации от одного человека другому (между субъектами информационных отношений) и человек передает информацию,

например, в виде устной речи, то для передачи таких сведений на большое расстояние необходимо речевой сигнал (акустический) преобразовать в электрический. Следует заметить, что содержание сведений при преобразовании сигналов не изменяется. Вместе с тем существует возможность преобразовать информацию из одной формы представления в другую. Например, текст на бумажном носителе с помощью сканера, подключенного к персональному компьютеру, можно преобразовать в электронный вид – файл, а потом с помощью принтера содержимое этого файла распечатать на бумаге и получить первоначальную форму представления информации.

Возвращаясь к преобразованию сигналов, необходимо отметить, что сигналы можно условно разделить на первичный и вторичный. Рассмотрим пример преобразования сигналов в телефонной связи (рис. 1.1). Посредством речевого аппарата человек формирует речевой (акустический) сигнал, который является первичным. Первичный сигнал формируется источником информации и является удобной для него формой представления, более того, только он может быть воспринят человеком. Этот сигнал распространяется через воздушную (газообразную) среду и преобразуется микрофоном телефонного аппарата в электрический сигнал. Электрический сигнал является вторичным сигналом. По сути, вторичный сигнал формируется путем преобразования первичного сигнала, его форма и параметры пригодны для распространения в определенной среде.

Необходимость преобразования сигналов обусловлена тем, что передать речевой (акустический) сигнал на значительное расстояние не представляется возможным из-за недостаточной его амплитуды, что, по сути, определяется пределом громкости речи человека. Иными словами, ввиду затухания сигнала в среде его распространения максимальное расстояние, на которое он может быть передан, будет определяться максимально предельным уровнем громкости речи человека. Именно поэтому речевой (акустический) сигнал преобразуют в электрический, так как для передачи такого сигнала можно создать передатчик с необходимым уровнем мощности и гарантированно передать информацию на значительно большее расстояние, чем расстояние, на которое передается речевой (акустический) сигнал, формируемый речевым аппаратом человека.

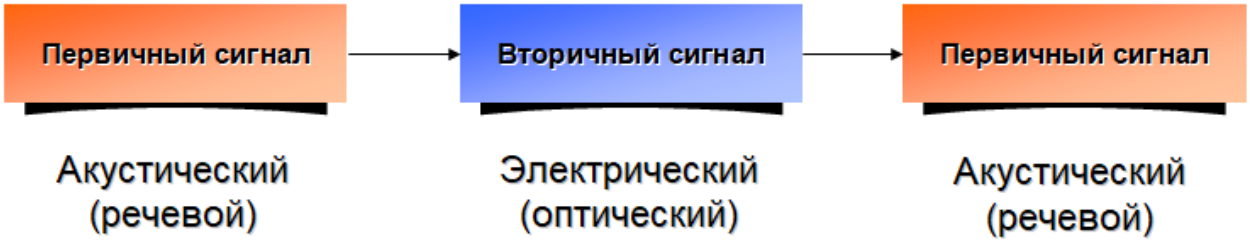


Рис. 1.1. Схематичное изображение преобразования сигналов при их передачи на большое расстояние

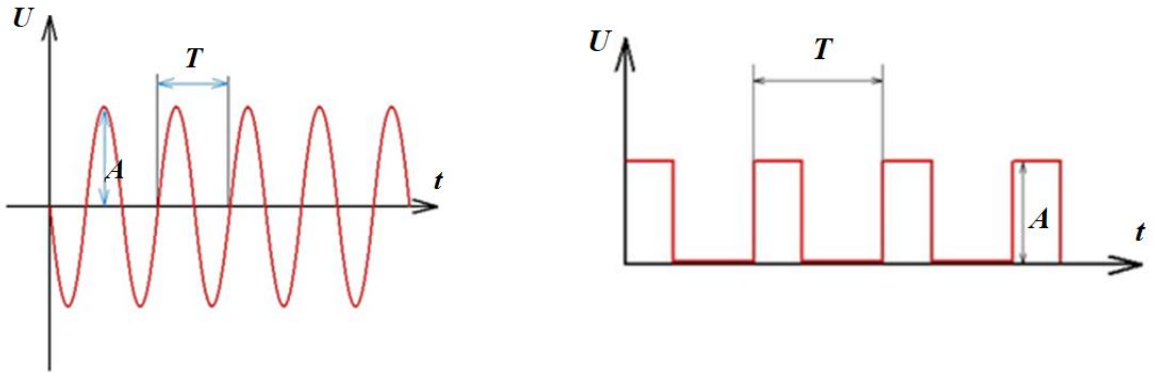
Возвращаясь к телефонной связи (см. рис. 1.1), нужно заметить, что электрический сигнал может быть преобразован в оптический. Необходимость та-

кого преобразования обусловлена в первую очередь снижением расходов на передачу информации на большие расстояния. Если выполнялось преобразование электрического сигнала в оптический, то на приемной стороне будет выполнено обратное преобразование, а именно оптического сигнала в электрический, и в конечном итоге электрический сигнал в телефонном аппарате абонента, который используется для его приема, будет преобразован, например динамической головкой, в речевой (акустический) сигнал.

Все виды сигналов делятся на две группы.

1. Аналоговый. Главное отличие этого сигнала – это непрерывность его значений (параметров) на временном отрезке его существования. На рис. 1.2, *а* схематично демонстрируется непрерывность изменения амплитуды (*A*) аналогового сигнала на периоде его наблюдения. Необходимо заметить, что человек способен формировать и воспринимать информацию, например речевую, только когда она представлена в виде аналогового сигнала.

2. Цифровой. У этого сигнала его значения (параметры) в отличие от аналогового сигнала дискретны (рис. 1.2, *б*). Преобразование аналогового сигнала в цифровой будет неизбежно снижать качество передаваемой информации в ходе таких преобразований. Вместе с тем этот процесс вполне управляемый. Поэтому можно задать критерии качества информации, которые необходимо получить, и выбрать соответствующие параметры аналого-цифрового преобразования. Преобразование аналоговых сигналов в цифровые призвано снизить воздействие различного рода помех на аналоговый сигнал, который передается по каналу связи, а соответственно, минимизировать искажение передаваемой информации. Искажения информации могут привести к невозможности ее идентифицировать, распознать, а следовательно, получить, а также повлиять на ее содержание.



а *б*

Рис. 1.2. Схематичное изображение аналогового (*а*) и цифрового (*б*) сигналов

Канал передачи информации. Передача информации организуется посредством канала связи (рис. 1.3). В качестве физической среды передачи информации в каналах связи выступают воздушная или кабельная линия связи. В качестве кабельных линий связи используют волоконно-оптические и линии связи с металлическими проводниками, соответственно, по ним могут распро-

страняться оптические и электрические сигналы. Необходимо заметить, что в канале связи на передаваемые сигналы всегда воздействуют помехи. Их влияние приводит к невозможности приема информации или ее искажению. Считается, что наиболее помехозащищенными являются волоконно-оптические линии связи, в том числе и поэтому прибегают к преобразованию электрических сигналов в оптические.

Рис. 1.3. Упрощенное изображение канала связи

Обработка и хранение информации в электронном виде. Процессы обработки и хранения информации в электронном виде непосредственно связаны с информационной системой. Сведения в данном случае представлены, например, в виде файлов, которые хранятся и обрабатываются с применением материальных носителей информации, которые, в свою очередь, являются физическими накопителями, например жесткий диск (HDD – Hard Disk Drive или SSD – Solid State Drive), а организованная на них файловая система позволяет записывать на них, хранить и читать файлы.

Информационная система. Информационные системы в различных организациях используются для поиска, получения, передачи, сбора, обработки, накопления, хранения информации. Рассмотрим каждый компонент информационной системы (рис. 1.4).

Хранение информации обеспечивается на материальных носителях, которые, как было отмечено выше, представлены дисковыми накопителями и организуются в дисковый массив, представляющий собой базу данных. Она позволяет обеспечить сбор, накопление и хранение информации. Для поиска информации в базе данных, а также для ее обработки, получения, передачи и использования необходима система управления базой данных. Объединение несколько баз данных в единую организационно-техническую их совокупность приводит к формированию банка данных. Для объединения баз данных в банк данных и обеспечения взаимодействия с ним пользователей необходим программно-технический комплекс, в состав которого входит оборудование и программное обеспечение, позволяющее организовать канал связи и взаимодействие между пользователем и банком данных.

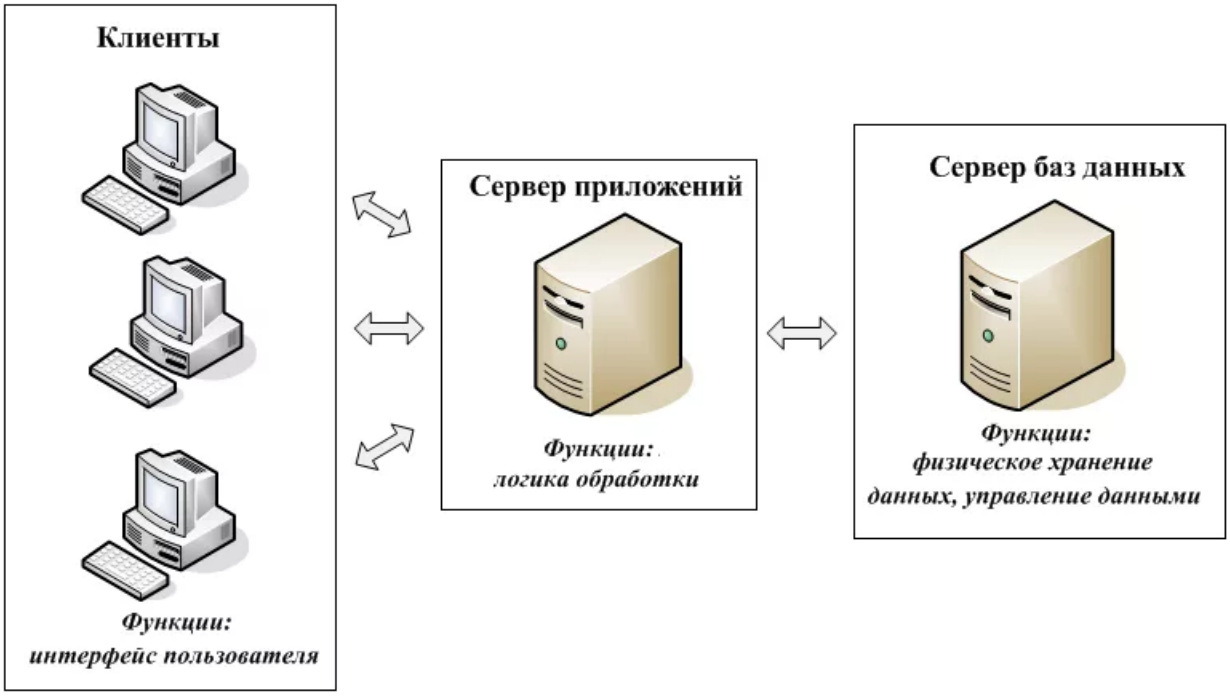


Рис. 1.4. Схематичное изображение информационной системы

Информационная технология. Для поиска, получения и передачи информации в базу данных пользователь должен обладать навыками пользования техническими средствами и установленным на них программным обеспечением. Графический интерфейс современных устройств (персональный компьютер, смартфон и т. п.), которые обеспечивают доступ к информационным системам, достаточно интуитивно понятный, и получение базовых навыков работы с ним не требует значительного времени. Вместе с тем необходимо отметить, что все сведения делятся на две группы:

1) общедоступная информация;

2) информация, распространение и (или) предоставление которой ограничено.

Это означает, что круг лиц, имеющих доступ к сведениям второй группы, ограничивается обладателем такой информации, и именно она подлежит защите от несанкционированного доступа. Для организации системы защиты информации требуются ресурсы: время, люди, программно-технические средства, финансовое обеспечение, а они всегда ограничены. Поэтому для экономии ресурсов необходимо выполнить классификацию информации, что позволит выделить важные для обеспечения бизнес-процессов обладателя сведения, подлежащие защите.

Уничтожение информации. Как было указано выше, хранение информации реализуется посредством дисковых накопителей, и объем сведений, которые они могут включать, конечен. Увеличение объема дискового пространства обеспечивается за счет увеличения числа накопителей, которые формируют массив дисковых накопителей – это ведет к увеличению стоимости такой си-

стемы хранения и стоимости ее обслуживания, например необходимо своевременно выполнять замену выработавших свой ресурс накопителей. Поэтому экономия объема дискового пространства может быть реализована за счет удаления ненужной и неактуальной информации. Следует заметить, что право на это имеет обладатель информации.

Контрольные вопросы

1. Что такое информация и зачем она нужна человеку?
2. Каким образом доверие к автору влияет на достоверность информации? Приведите пример.
3. Каким образом взаимосвязаны доверие к источнику информации и достоверность информации? Приведите пример.
4. Какие ключевые отличия оценки и факта? Назовите и поясните наиболее существенные из них.
5. По результатам проверки достоверности информации установлено, что только части сведений можно доверять. Каковы ваши дальнейшие действия?
6. В чем различие между предоставлением и представлением информации?
7. Какие выделяют виды сигналов?
8. Почему необходимо преобразовывать сигналы?
9. Что такое информационная технология?
10. Чем обусловлена необходимость уничтожения информации?

2. ИНФОРМАЦИЯ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ И ЕЕ ДЕМАСКИРУЮЩИЕ ПРИЗНАКИ

Основная терминология темы [1–3]. **Государственные секреты** – сведения, защищаемые государством в соответствии Законом Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах» и другими актами законодательства Республики Беларусь.

Гриф секретности – реквизит, проставляемый на носителе государственных секретов и (или) сопроводительной документации к нему, свидетельствующий о степени секретности содержащихся на этом носителе государственных секретов.

Демаскирующие признаки – характеристики любого рода, поддающиеся обнаружению и анализу и являющиеся источником информации об объекте.

Допуск к государственным секретам – право гражданина Республики Беларусь, иностранного гражданина, лица без гражданства или государственного органа, иной организации на осуществление деятельности с использованием государственных секретов.

Доступ к государственным секретам – ознакомление гражданина с государственными секретами или осуществление им иной деятельности с использованием государственных секретов.

Доступ к информации – возможность получения информации и пользования ею.

Коммерческая тайна – сведения любого характера (технического, производственного, организационного, коммерческого, финансового и иного), в том числе секреты производства (ноу-хау), соответствующие требованиям Закона Республики Беларусь от 5 января 2013 г. № 16-З «О коммерческой тайне», в отношении которых установлен режим коммерческой тайны.

Обладатель информации – субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства Республики Беларусь, или по договору.

Персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

Распространение информации – действия, направленные на ознакомление с информацией неопределенного круга лиц.

Служебная информация ограниченного распространения – сведения, касающиеся деятельности государственного органа, юридического лица, распространение и (или) предоставление которых могут причинить вред национальной безопасности Республики Беларусь, общественному порядку, нравственности, правам, свободам и законным интересам физических лиц, в том числе их чести и достоинству, личной и семейной жизни, а также правам и законным интересам юридических лиц и которые не отнесены к государственным секретам.

Степень секретности – показатель важности государственных секретов, определяющий меры и средства защиты государственных секретов.

Классификация информации. Для обеспечения защиты информации необходимо обладать определенными ресурсами (наличие компетентных специалистов, финансовые средства, средства защиты информации и т. д.), которые независимо от масштаба организации (насколько она крупная) всегда ограничены. Поэтому для эффективного и экономного использования ресурсов необходимо принять решение о том, какую информацию требуется защищать (определить перечень сведений, подлежащих защите), исходя из чего существующую в организации информацию следует классифицировать, т. е. из всего объема сведений нужно выделить те, которые подлежат защите.

Классификация информации выполняется специалистами по защите информации (т. е. теми людьми, которые эту защиту будут обеспечивать). Для этого используются нормативные правовые акты, которые устанавливают порядок обеспечения защиты информации. По результатам такой деятельности специалист по защите информации составляет перечень сведений, подлежащих защите, который утверждается руководителем организации.

Одним из нормативных правовых актов, который используется при классификации информации, является Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (далее – Закон № 455-З). В соответствии с Законом № 455-З в зависимости от категории доступа выделяют:

– общедоступную информацию;

– информацию, распространение и (или) предоставление которой ограничено.

К общедоступной информации относится информация, доступ к которой, распространение и (или) предоставление которой не ограничены. В соответствии с Законом № 455-З общедоступная информация – это:

– информация о правах, свободах, законных интересах и обязанностях физических лиц, правах, законных интересах и обязанностях юридических лиц и о порядке реализации прав, свобод и законных интересов, исполнения обязанностей;

– информация о деятельности государственных органов, общественных объединений;

– информация о правовом статусе государственных органов, за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;

– информация о социально-экономическом развитии Республики Беларусь и ее административно-территориальных единиц;

– информация о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;

– информация о состоянии здравоохранения, демографии, образования, культуры, сельского хозяйства;

– информация о состоянии преступности, а также о фактах нарушения законности;

– информация о льготах и компенсациях, предоставляемых государством физическим и юридическим лицам;

– информация о размерах золотого запаса;

– информация об обобщенных показателях по внешней задолженности;

– информация о состоянии здоровья должностных лиц, занимающих должности, включенные в перечень высших государственных должностей Республики Беларусь;

– информация, накапливаемая в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

К информации, распространение и (или) предоставление которой ограничено, относится:

– информация о частной жизни физического лица и персональные данные;

– сведения, составляющие государственные секреты;

– служебная информация ограниченного распространения;

– информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну;

– информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;

– иная информация, доступ к которой ограничен законодательными актами.

Рассмотрим подробнее перечисленные виды информации, распространение и (или) предоставление которой ограничено.

В соответствии с Законом Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» выделяют:

– общедоступные персональные данные;

– специальные персональные данные.

Общедоступные персональные данные – персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов. Из представленного определения следует, что можно выделить три условия, при которых персональные данные становятся общедоступными. Первое условие – распространение персональных данных самим их субъектом, т. е. физическим лицом, к которому относятся эти данные. Пример реализации этого условия – размещение пользователем на своей странице в социальной сети сопровождаемых соответствующими комментариями фотографий, сделанных в автосалоне, в котором он приобрел себе новый автомобиль, или в офисе, в котором расположено его новое рабочее место. Второе условие – распространение персональных данных с разрешения их субъекта. Пример реализации этого условия – размещение пользователем на своей странице в социальной сети сопровождаемых соответствующими комментариями фотографий, на которых он запечатлен

со своим братом, при условии, если брат дал на это разрешение. Третье условие – распространение персональных данных в соответствии с нормами законодательных актов. Пример реализации этого условия – обнародование биографических данных кандидатов в депутаты в период предвыборной кампании в соответствии с требованиями Избирательного кодекса Республики Беларусь.

Специальные персональные данные – персональные данные, касающиеся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности, а также биометрические и генетические персональные данные. Из представленного определения видно, что во множество специальных персональных данных входят подмножества, которые называют биометрическими и генетическими персональными данными.

Биометрические персональные данные – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и др.).

Генетические персональные данные – информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца.

В соответствии со ***ст. 17 Закона № 455-З*** вторая категория информации, распространение и (или) предоставление которой ограничено, – ***государственные секреты.*** Деятельность в области защиты государственных секретов регламентируется ***Законом Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах» (далее – Закон № 170-З)***.

Особенностью данной категории информации является то, что обладателем ее является государство – Республика Беларусь. Эта информация для любого государства является наиболее приоритетной из всех существующих категорий сведений, ввиду того, что она значительно влияет на все сферы его жизнедеятельности. Как известно, государства существуют в условиях сильной конкуренции, возникающей между ними, поэтому для того, чтобы обойти конкурента, быть лучше его в какой-либо сфере, необходимо принять управленческое решение, а для этого нужна достоверная, полная и своевременная информация, которой на уровне различных стран являются их государственные секреты.

К государственным секретам могут быть отнесены следующие сведения:

– в области политики;

– области экономики и финансов;

– области науки и техники;

– области разведывательной, контрразведывательной и оперативно-розыскной деятельности;

– информационной и иных областях национальной безопасности Республики Беларусь;

– иные сведения из указанных областей, которые включаются в перечень сведений, подлежащих отнесению к государственным секретам.

Сведения, которые могут быть отнесены к государственным секретам, определены в ***ст. 14 Закона № 170-З.***

Государственные секреты делятся на две категории:

1) государственная тайна – сведения, в результате разглашения или утраты которых могут наступить ***тяжкие последствия*** для национальной безопасности Республики Беларусь;

2) служебная тайна – сведения, в результате разглашения или утраты которых может быть причинен ***существенный вред*** национальной безопасности Республики Беларусь.

Допускается, что вторая категория (служебная тайна) может являться составной частью первой категории (государственной тайны), не раскрывая ее в целом.

Как можно заметить, определения терминов «государственная тайна» и «служебная тайна» разнятся буквально в трех словах. В контексте этих определений следует рассмотреть определение термина «национальная безопасность». Оно фигурирует в Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575. Под национальной безопасностью следует понимать состояние защищенности *национальных интересов* Республики Беларусь от внутренних и внешних *угроз*. В представленном определении выделены курсивным начертанием два термина, которым следует уделить внимание. Под *национальными интересами* следует понимать совокупность потребностей государства по реализации сбалансированных интересов личности, общества и государства (рис. 2.1).

Рис. 2.1. Объекты национальной безопасности

Под *угрозой национальной безопасности* следует понимать потенциальную или реально существующую возможность нанесения ущерба национальным интересам Республики Беларусь.

На документах, содержащих государственные секреты, проставляются следующие грифы секретности: «Особой важности», «Совершенно секретно» и «Секретно» (рис. 2.2).

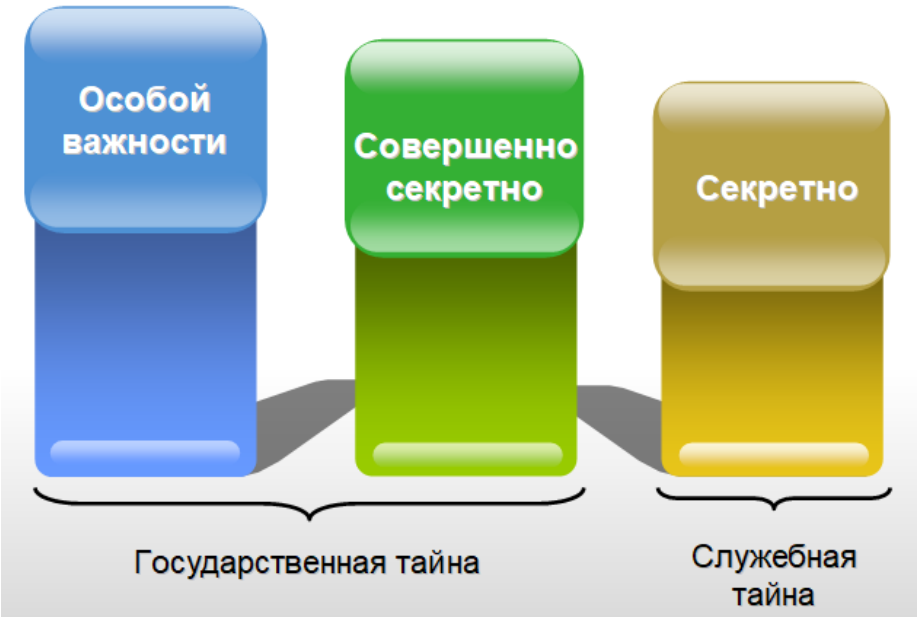


Рис. 2.2. Соотношение грифов секретности и категорий государственных секретов

Под грифом секретности следует понимать реквизит, проставляемый на носителе государственных секретов и (или) сопроводительной документации к нему, свидетельствующий о степени секретности содержащихся на этом носителе государственных секретов.

Для организации деятельности, связанной с контролем доступа к государственным секретам (определением правил доступа человека к такой категории информации), и с учетом того, что сведения представлены в определенной форме и на определенных носителях, выполняется маркировка последних. Маркировка подразумевает указание ***грифа секретности*** информации, которая содержится на носителе. Гриф по своей сути и определяет степень секретности информации.

Разработанная система категорий государственных секретов и ранжирование их важности посредством грифов секретности позволяют обеспечить контроль доступа к такой информации и минимизировать ее утечку.

Для получения допуска лица к государственным секретам необходимо, чтобы в организации были выполнены следующие условия:

1. Наличие в структуре организации подразделения, обеспечивающего защиту государственных секретов (допускается заключение договора на оказание такой услуги сторонней организацией).

2. Существует номенклатура должностей сотрудников, которые подлежат допуску к государственным секретам.

3. Руководитель подразделения, обеспечивающего защиту государственных секретов, имеет допуск к этой категории информации.

4. Приняты меры по защите государственных секретов в соответствии с законодательством Республики Беларусь.

Приведем пример основных условий, выполнение которых позволяет предоставить допуск гражданину к государственным секретам.

1. Гражданин ознакомлен с законодательными актами, которые регламентируют ответственность за нарушение законодательства о защите государственных секретов и временное ограничение прав в соответствии ***со ст. 41 Закона № 170-З***.

2. Получено от гражданина письменное согласие на проведение в отношении его проверочных мероприятий.

3. Гражданин предоставил свои персональные данные.

4. Имеется документ, свидетельствующий о согласовании уполномоченным государственным органом по защите государственных секретов предоставления гражданину допуска.

5. Проведены проверочные мероприятия в отношении гражданина, которому необходимо предоставить допуск к государственным секретам.

Как было отмечено выше, при допуске к государственным секретам действуют временные ограничения прав человека (на время допуска к государственным секретам):

1) в период проведения проверочных мероприятий;

2) в праве свободного выезда за границу;

3) в праве получения от иностранного государства любых привилегий и льгот.

Человек, который получил ***допуск*** к государственным секретам и, исходя из чего, ознакомился с ними, фактически получил ***доступ*** к государственным секретам.

Государственное управление и регулирование деятельности в сфере государственных секретов обеспечивается соответствующими государственными учреждениями и должностными лицами (рис. 2.3).

Кратко рассмотрим основные полномочия участников системы государственного управления и регулирования в сфере государственных секретов.

Президент Республики Беларусь – определяет государственную политику, создает и реорганизует уполномоченные в сфере защиты государственных секретов государственные органы (***ст. 4 Закона № 170-З***).

Совет Министров Республики Беларусь – организует разработку законодательства и проектов государственных программ в сфере государственных секретов (***ст. 5 Закона № 170-З***).

Межведомственная комиссия по защите государственных секретов при Совете Безопасности Республики Беларусь – координирует деятельность

государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам (***ст. 6 Закона № 170-З***).

Уполномоченный государственный орган по защите государственных секретов – обеспечивает координирование деятельности государственных органов и иных организаций по защите государственных секретов (***ст. 7 Закона № 170-З***).

Органы государственной безопасности – обеспечивают координирование применения средств шифрованной, других видов специальной связи, использование средств криптографической защиты информации и осуществляют контроль за защитой государственных секретов (***ст. 8 Закона № 170-З***).

Оперативно-аналитический центр при Президенте Республики Беларусь – обеспечивает координирование деятельности по технической защите государственных секретов (***ст. 9 Закона № 170-З***).

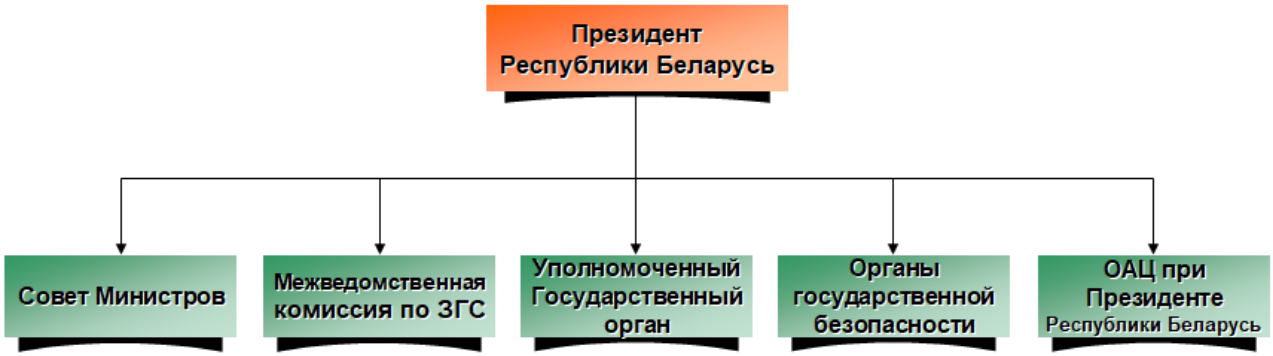


Рис. 2.3. Государственные учреждения и должностные лица, обеспечивающие управление и регулирование в сфере государственных секретов

Перечень сведений, относящихся к **служебной информации ограниченного распространения**, представлен в постановлении Совета Министров Республики Беларусь от 12 августа 2014 г. № 783. Эти сведения разделены на следующие группы:

1) мобилизационные вопросы:

– договоры о выполнении мобилизационных заданий на поставку товаров;

– сведения о мобилизационной подготовке;

2) наука и техника, научно-техническая информация:

– сведения о конкретных разработчиках вооружения;

– сведения о структурных схемах автоматизированных систем управления;

– сведения об экспорте (импорте) результатов научно-технической деятельности, которые могут быть использованы при создании продукции военного назначения и т. п.;

3) оборона и государственная безопасность:

– сведения о методах подготовки и проведения террористических актов;

– сведения о состоянии подразделений радиоэлектронной разведки и средствах связи;

– сведения об органах пограничной службы и внутренних войск Министерства внутренних дел;

– сведения об объектах информатизации, включенных в Государственный реестр критически важных объектов информатизации (включая сведения о системах информационной безопасности таких объектов) и т. п.;

4) вопросы гражданской обороны, предупреждения и ликвидации чрезвычайных ситуаций, заимствования материальных ценностей:

– сведения о центрах управления опасными производствами;

– сведения о порядке физической защиты объектов, представляющих повышенную техногенную и экологическую опасность и т. п.;

5) военно-техническое сотрудничество:

– сведения о содержании, подготовке, заключении и выполнении договоров, соглашений в сфере военно-технического сотрудничества;

– сведения об экспорте (импорте), объемах выпуска и поставках (в стоимостном и натуральном выражении) продукции военного назначения;

– сведения о зарубежных командировках сотрудников республиканских органов государственного управления по вопросам военно-технического сотрудничества и т. п.;

6) правоохранительная деятельность:

– сведения, связанные с профессиональной деятельностью, разглашение которых может создать угрозу личной безопасности сотрудников правоохранительных органов и членов их семей, их имуществу;

– сведения о силах, средствах, формах и методах ведения предварительного расследования;

– сведения о задачах, стоящих перед органами прокуратуры и т. п.;

7) промышленность:

– сведения о фондах заработной платы, количестве и обеспеченности специалистами предприятий, задействованных в производстве, и разработке продукции военного назначения;

– сведения о местах хранения, системе охраны, наличии и количестве оружия и боеприпасов, взрывчатых веществ, применяемых для производственных нужд и т. п.;

8) энергетика:

– сведения о количестве, точном местонахождении и емкости подземных хранилищ нефти, нефтепродуктов, газа;

– схемы отводов нефтепроводов и газопроводов, питающих электростанции;

– схемы внешнего электроснабжения электрифицируемой железной дороги и т. п.;

9) геология, полезные ископаемые, их добыча и переработка:

– сведения о технологиях получения из руды бериллия, лития;

– сведения о промышленных мощностях по производству радиоактивных элементов и т. п.;

10) транспорт:

– сведения о технических характеристиках метрополитена;

– сведения о перевозках любыми видами транспорта валютных ценностей, драгоценных металлов и драгоценных камней, денежных знаков;

– сведения о дислокации воинских погрузочно-разгрузочных устройств и т. п.;

11) связь:

– сведения о расписании движения автомобилей, перевозящих денежные средства, по почтовым маршрутам;

– сведения о количественном и персональном составе сотрудников Государственной фельдъегерской службы Республики Беларусь;

– опознавательные сигналы и позывные радиостанций государственных органов и т. п.;

12) внешнеэкономическая деятельность, финансы:

– сведения, связанные с внешним государственным долгом Республики Беларусь;

– сведения о торгово-экономических вопросах военно-технического сотрудничества;

– сведения о размерах, состоянии и формировании Государственного фонда драгоценных металлов и драгоценных камней Республики Беларусь и т. п.;

13) банковская деятельность:

– сведения об эскизных проектах, степени и элементах защиты наличных денежных средств Республики Беларусь нового образца;

– сведения о плановых и фактических объемах производства и объемах выпуска в обращение наличных денежных средств Национального банка;

– сведения об организации, методах и средствах комплексной защиты информации от несанкционированного доступа и утечки по техническим каналам, применяемых в Национальном банке, банках и небанковских кредитно-финансовых организациях и т. п.;

14) геодезия, картография:

– государственные топографические карты масштабов 1:200 000 и 1:100 000;

– сведения о плановых координатах геодезических пунктов, определенные с точностью грубее 1 метра и до 50 метров включительно и т. п.;

15) гидрометеорология:

– сведения о координатах гидрометеорологических станций и постов;

– сводные сведения об обеспечении гидрометеорологической информацией Вооруженных Сил Республики Беларусь и т. п.;

16) медико-санитарные вопросы:

– сведения о новых медицинских средствах противорадиационной, противохимической и противобактериологической защиты войск, населения и животных;

– сведения об объемах производства наркотических средств, психотропных веществ и их прекурсоров, ввоза их в Республику Беларусь из конкретной страны и вывоза в конкретную страну и т. п.

На документах, содержащих служебную информацию ограниченного распространения, проставляется ограничительный гриф «Для служебного пользования».

В соответствии со ст. 5 Закона Республики Беларусь от 5 января 2013 г. № 16-З «О коммерческой тайне» режим **коммерческой тайны** может устанавливаться в отношении сведений, которые одновременно соответствуют следующим требованиям:

– не являются общеизвестными или легкодоступными третьим лицам в тех кругах, которые обычно имеют дело с подобного рода сведениями;

– имеют коммерческую ценность для их обладателя в силу неизвестности третьим лицам;

– не являются объектами исключительных прав на результаты интеллектуальной деятельности (исключительное право позволяет его обладателю распоряжаться результатом интеллектуальной деятельности);

– не отнесены в установленном порядке к государственным секретам.

Сведения имеют коммерческую ценность в случае, если обладание ими позволяет лицу при существующих или возможных обстоятельствах увеличить доходы, сократить расходы, сохранить положение на рынке товаров, работ или услуг либо получить иную коммерческую выгоду.

Обратите внимание на то, что необходимость отнесения сведений к информации, распространение и (или) предоставление которой ограничено (в данном случае – к коммерческой тайне), обусловлено ущербом, который может быть нанесен организации в случае ее разглашения.

Рассмотрим пример. Некоторой организацией объявлен тендер на закупку некоторого оборудования, и информация о технических характеристиках оборудования, которое требуется купить, размещена на специализированном сайте по закупкам. В тендере решили принять участие два поставщика. Они способны продать необходимую организации технику. Обе организации формируют свои предложения, в которых как у одного поставщика, так и у другого указана одинаковая техника. Для того чтобы выиграть тендер и получить деньги при продаже техники, необходимо каждому из поставщиков указать такую цену, которая бы покрыла его расходы и принесла прибыль, но в то же время была бы меньше, чем у поставщика-конкурента. Предположим, что первый поставщик определил эту цену и представил соответствующий документ организации, которая объявила тендер. По просьбе второго поставщика один из сотрудников организации, в которую закупается оборудование, предоставил ему информацию о том, какую цену обозначил первый поставщик. На основании этого второй поставщик сформировал свое предложение по цене ниже, чем у первого поставщика. В случае если условия поставки у первого и второго поставщика одинаковы, то решение на закупку может быть принято по критерию наименьшей цены. Соответственно, первый поставщик проиграет тендер и не получит денежные средства, которые он рассчитывал получить при условии победы в тендере. Таким образом, неполученные средства можно рассматривать как

ущерб, обусловленный недобросовестной конкуренцией второго поставщика при участии сотрудника организации, объявившей тендер.

Проблема, изложенная в примере, могла бы быть решена, если бы в организации, объявившей тендер, приняли бы необходимые меры для ограничения доступа к информации, которая поступила от первого поставщика. Очень часто разглашение информации связано с тем, что классификация ее не выполнена и, соответственно, необходимые меры по ее защите не реализованы. Поэтому классификация информации – это первый шаг к обеспечению ее защиты.

Под профессиональной тайной следует понимать сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией и законами Республики Беларусь. В первую очередь к профессиональной тайне относят информацию о частной жизни физического лица, которая доверяется представителям некоторых профессий (врачам, психологам, адвокатам, нотариусам, работникам служб ЗАГС, священнослужителям и т. п.) для того, чтобы те смогли выполнить свои профессиональные обязанности.

В соответствии со ст. 121 Банковского кодекса Республики Беларусь, **банковская тайна** – это сведения о счетах и вкладах (депозитах), в том числе о наличии счета в банке (небанковской кредитно-финансовой организации), его владельце, номере и других реквизитах счета, размере средств, находящихся на счетах и во вкладах (депозитах), а равно сведения о конкретных сделках, об операциях без открытия счета, операциях по счетам и вкладам (депозитам), а также об имуществе, находящемся на хранении в банке.

На рис. 2.4 представлена схема, на которой отражены наименования рассмотренных видов информации, распространение и (или) предоставление которой ограничено, а также наименования документов, в которых детально изложен порядок обращения с такой информацией.

Демаскирующие признаки и их классификация. В современном мире часто обсуждается «анонимность пользователя» сети Интернет. Необходимо отметить, что, исходя из многообразия персональных данных, а также других идентификаторов человека как пользователя программно-технических средств, подключенных к сети передачи данных, обеспечение его анонимности является крайне сложной задачей. Это обусловлено множеством признаков, совокупность которых позволит его обнаружить и идентифицировать. Такие признаки называются *демаскирующими*. Именно по ним выполняется обнаружение и идентификация различных объектов. Для реализации таких процессов сначала нужно получить совокупность признаков объекта, который необходимо идентифицировать, а затем выполнить их поиск. Рассмотрим пример. Для поиска требуемой информации человек прибегает к использованию некоторой поисковой системы, а взаимодействует с нею используя браузер. Поиск объекта интереса он реализует формируя запрос, в котором указывает, по сути, демаскирующие признаки объекта.

Зная характеристики объекта, можно составить совокупность демаскирующих признаков (рис. 2.5), последующее использование которых позволит его идентифицировать среди объектов одного класса.

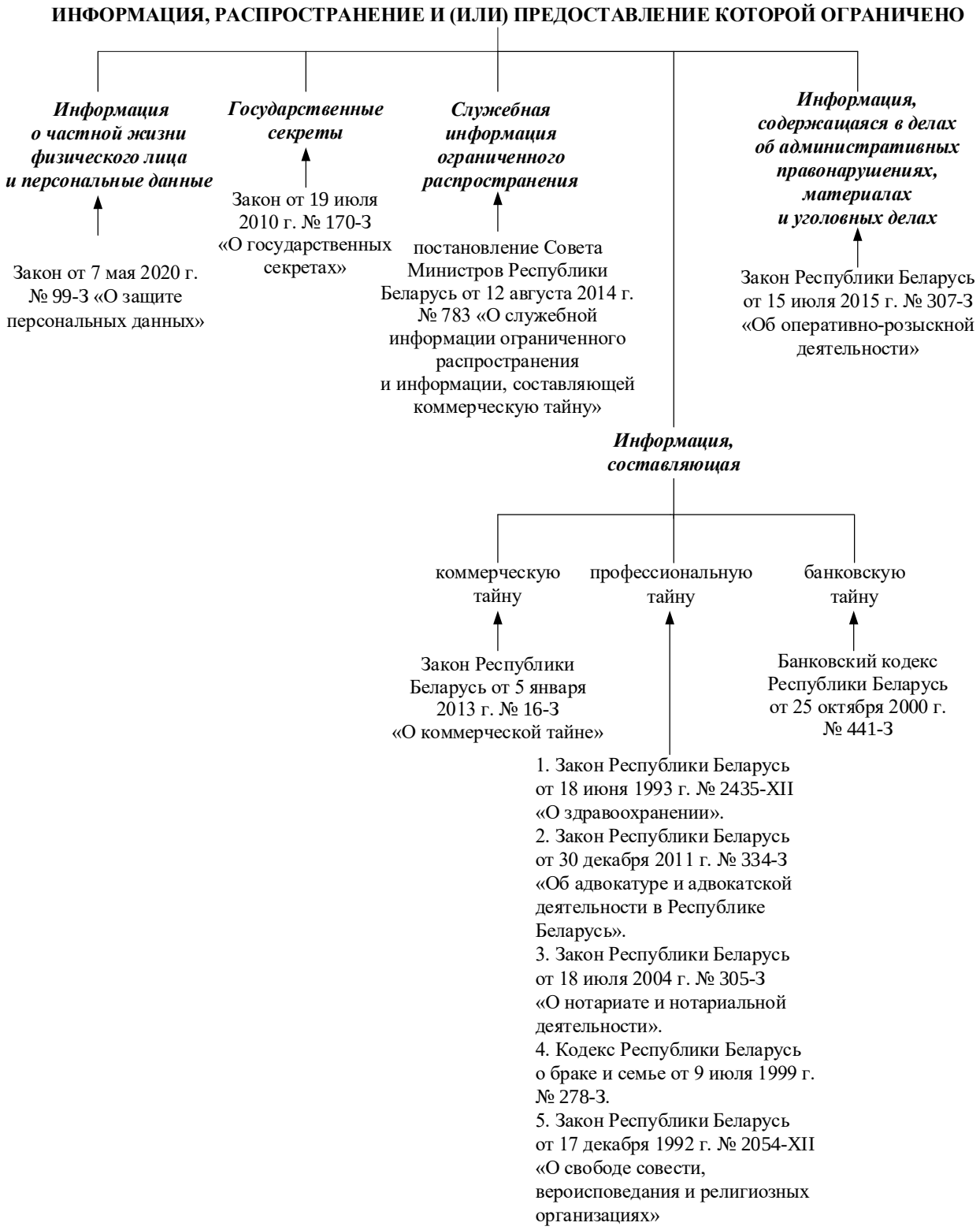


Рис. 2.4. Виды информации, распространение и (или) предоставление которой ограничено, и наименования связанных с ними нормативных правовых актов

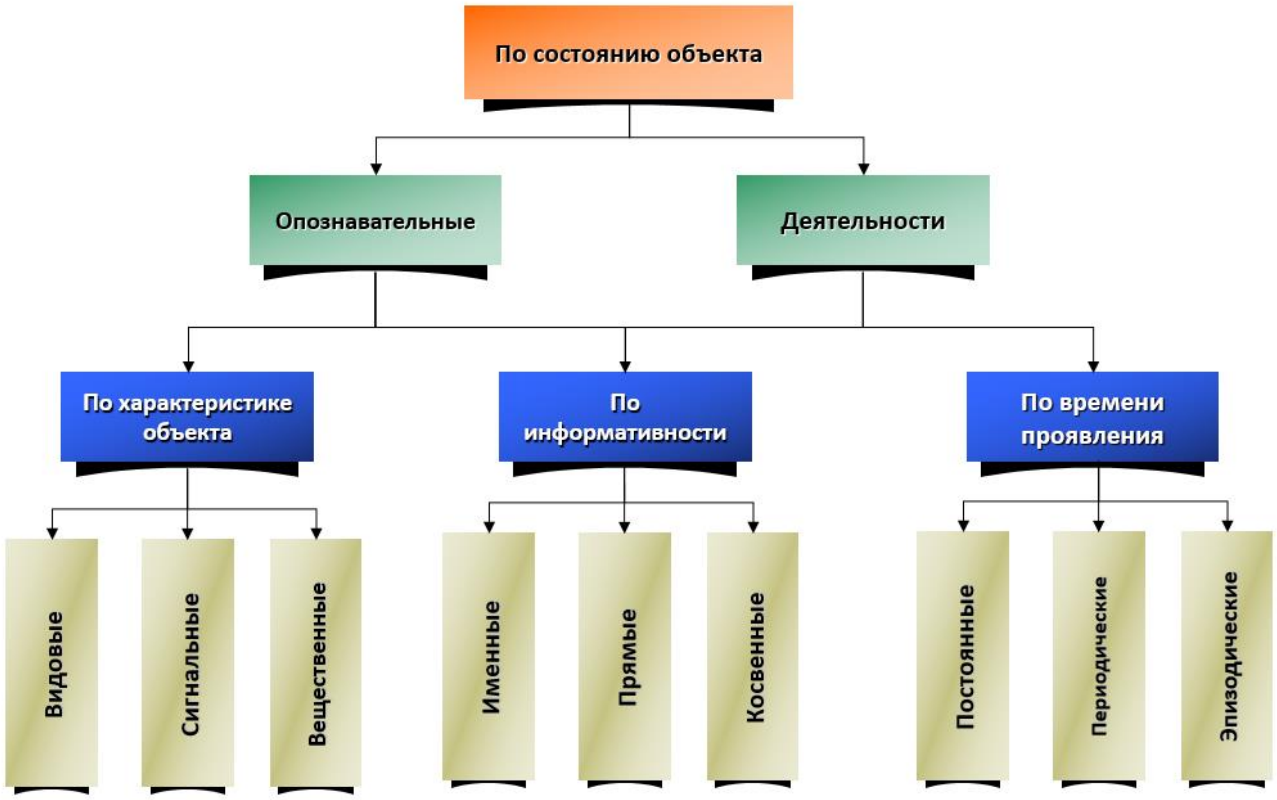


Рис. 2.5. Классификация демаскирующих признаков объекта

Опознавательные демаскирующие признаки характеризуют физические свойства объекта в статическом состоянии:

– внешний вид (цвет, форма, размер);

– физические свойства (масса, плотность, вязкость, проводимость);

– химические свойства (химический состав материала).

Демаскирующие признаки деятельности описывают последовательность событий во времени, или действий составных элементов объекта, или объекта в целом и взаимодействующих с ним других объектов, характеризуют этапы и режимы функционирования объекта (скорость, упругость ударов и т. д., т. е. изменения статистических свойств объекта во времени).

По характеристикам объекта демаскирующие признаки принято подразделять:

– на видовые (форма объекта, его размеры, детали объекта, тон, цвет, структура поверхности и т. д.);

– сигнальные (параметры физических полей и электрических сигналов, создаваемых объектом (амплитуда, частота, фаза, вид модуляции сигнала));

– вещественные (физический и химический состав, структура и свойства вещества, из которого состоит объект).

По информативности демаскирующие признаки делят:

– на именные (фамилия, имя, отчество человека, его биометрические характеристики, инвентарный номер прибора или мебели и т. д.). Главная особенность таких признаков – они обеспечивают вероятность идентификации объек-

та, близкую к 1 (значение вероятности изменяется от 0 до 1: значение вероятности 1 свидетельствует о том, что событие обязательно произойдет, а 0 – обязательно не произойдет). Поэтому в случае использования именных демаскирующих признаков ошибка идентификации объекта снижается;

– прямые (непосредственно принадлежащие определенному классу объекта. Вероятность идентификации объекта по такому признаку изменяется в пределах от 0 до 1). Так, например, у автомобиля есть кузов и колеса, а у человека – туловище, голова, руки и ноги;

– косвенные (непосредственно не принадлежащие объекту, но отражающие его свойства и состояние. Они позволяют повысить точность идентификации объекта). Например, по наличию тени, которая создается объектом, можно судить о его местоположении и даже форме.

В основу классификации заложен принцип оценки количества информации, которую можно получить в результате обнаружения демаскирующего признака объекта. Чем более уникален признак (чем меньше объектов реального мира им характеризуется), тем большую информативность он имеет. Наиболее информативны именные признаки, характерные только для конкретного типа объектов.

По времени проявления признаки разделяют:

– на постоянные (не изменяющиеся или незначительно изменяющиеся в течение жизненного цикла объекта);

– периодические (наблюдающиеся с определенной частотой (периодичностью));

– эпизодические (проявляющиеся при определенных условиях).

Рассмотрим изображение на рис. 2.6 и составим по нему совокупность демаскирующих признаков, используя их классификацию, представленную на рис. 2.5.

Рис. 2.6. Внешний вид некоторого объекта

Мы используем только изображение объекта, поэтому начнем его анализ с видовых демаскирующих признаков, так как для их формирования необходим внешний вид объекта.

К видовым и одновременно прямым демаскирующим признакам объекта можно отнести следующие: голова, туловище, руки и ноги. Опираясь на эти признаки, можно заключить, что объект – представитель одного из классов животного мира. Форма этого объекта (взаимное расположение его головы, туловища, рук и ног) также является видовым демаскирующим признаком, опираясь на который, можно сделать вывод, что объект является человеком. То, что объект стоит на ногах, является косвенным демаскирующим признаком, подтверждающим вывод о том, что это человек.

На туловище, части рук и на ногах у объекта надета одежда. В частности, штаны и футболка. Эти предметы одежды мы идентифицировали по их видовым демаскирующим признакам. Вместе с тем одежда – это косвенный демаскирующий признак того, что на изображении человек.

Все рассмотренные признаки, кроме положения объекта (стоит на ногах), являются постоянными. Именно поэтому можно идентифицировать объект. Это однозначно человек. Как известно, человек может лежать и сидеть, поэтому текущее его положение в пространстве – это периодический демаскирующий признак.

Демаскирующие признаки, которые мы указали выше, относятся к опознавательным демаскирующим признакам, так как мы имеем дело со статическим объектом (неподвижным изображением). Если бы у нас был видеофильм, где был бы запечатлен человек в некотором движении, то мы смогли бы указать еще и признаки деятельности.

Вместе с тем в качестве демаскирующего признака деятельности человека можно отметить такой сигнальный демаскирующий признак, как речь.

Совокупность отмеченных выше демаскирующих признаков позволяет идентифицировать объект, в данном случае человека. Если бы нам необходимо было установить его личность, то это потребовало бы наличия уже именных демаскирующих признаков, которые на данном изображении отсутствуют.

Следует отметить, что идентификация окружающих человека объектов (транспортные средства, объекты животного и растительного мира и т. д.) выполняется за счет анализа их признаков (демаскирующих признаков). Если совокупность демаскирующих признаков будет уникальна (не будет повторяться), то можно их использовать для идентификации объекта. Идентификация объекта позволяет установить его принадлежность к определенному классу, виду или типу.

Контрольные вопросы

1. Чем обусловлена необходимость классификации информации?
2. Каким образом выполняется классификация информации?

3. Что относится к информации, распространение и (или) предоставление которой ограничено?

4. В соответствии с какими нормативными правовыми актами выполняется классификация информации? Дайте пояснения по каждому нормативному правовому акту в части его использования при выполнения этой процедуры.

5. В чем различие между предоставлением и распространением информации?

6. Что такое демаскирующие признаки объекта и на какие категории они делятся?

7. В чем заключается различие между опознавательными демаскирующими признаками и признаками деятельности объекта? Приведите пример для конкретного класса объекта.

8. Какие демаскирующие признаки объекта относятся к именным демаскирующим признакам и в чем отличие их от прямых демаскирующих признаков? Приведите пример для конкретного класса объекта.

9. Оцените значимость косвенных демаскирующих признаков при идентификации объекта.

10. При каких условиях можно составить демаскирующие признаки деятельности объекта?

3. МОДЕЛЬ НАРУШИТЕЛЯ

Основная терминология темы [1, 2]. **Защита информации** – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Информационная сеть – совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи.

Информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах.

Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

Контролируемая зона – территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа.

Нарушитель безопасности информации – физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах.

Объект информационной инфраструктуры – критически важные объекты информатизации, информационные сети, информационные системы, информационные ресурсы и иные совокупности технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации.

Сеть электросвязи – технологическая система, включающая в себя средства электросвязи и линии электросвязи.

Средства криптографической защиты информации – технические, программные, программно-аппаратные средства, которые реализуют криптографические алгоритмы и протоколы, а также функции управления криптографическими ключами, механизмы идентификации и аутентификации.

Средства технической защиты информации – имеют техническую, программную или программно-аппаратную реализацию.

Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Характеристики нарушителя. В соответствии с определением нарушителем безопасности информации (далее – нарушитель) может быть не только постороннее лицо, т. е. не сотрудник организации, но и ее сотрудник. Рассмотрим основные характеристики нарушителя.

1. Цель. Процесс деятельности человека направлен на ожидаемый им ***результат***. Исходя из цели, выбираются методы и средства ее достижения. Вместе с тем человек случайно может совершать действия в информационной системе, которые впоследствии могут позволить отнести его к категории нарушителя. Например, иногда люди неосознанно (по невнимательности) удаляют файлы, которые им нужны. При таком стечении обстоятельств деятельность человека не целенаправленная.

2. Мотивация. Выполнение человеком некоторых действий, например воздействие на информационную систему, обусловлено тем, что у него есть некоторая потребность, которую ему необходимо удовлетворить, а соответственно, есть интерес к чему-то, поэтому он начинает действовать. Например, нарушитель, проводит кибератаку на информационную систему, и это даст ему возможность получить доступ к денежным средствам, а соответственно, удовлетворить некоторую свою, например, физиологическую потребность (в еде, в одежде и т. п.). Исходя из чего, мотивация – ***психофизиологический процесс, управляющий поведением человека***, определяющий его направленность, организованность и активность.

3. Финансовое обеспечение. Сюда относятся денежные средства, которые позволят нарушителю покрыть его затраты, которые будут сопряжены с его деятельностью. Например, для проведения кибератаки нарушителю необходимы программно-аппаратные средства, которые надо ему приобрести, а для этого нужны денежные средства.

4. Техническое обеспечение. Сюда относятся средства, которые позволят нарушителю реализовать запланированные действия и достичь своей цели. Указанные выше программно-технические средства относятся к техническому обеспечению деятельности нарушителя.

5. Наличие и уровень профессиональной подготовки. Для выполнения действий нарушителю, особенно с использованием соответствующего технического обеспечения, требуются соответствующие навыки пользования, например, программно-техническими средствами, а также пригодность этих навыков для достижения им своей цели. Так, например, наличие персонального компьютера у человека абсолютно не свидетельствует о том, что человек имеет навыки его настройки и использования для реализации кибератак.

6. Наличие и качество предварительной подготовки. Для достижения цели нарушитель будет вынужден планировать свои действия, выбирать необходимое техническое обеспечение и т. п. Таким образом, наличие и качество предварительной подготовки действий нарушителя определяют качество планирования мероприятий по достижению поставленной цели и возможность ее достижения.

7. Наличие и уровень внедрения на объект – определяет требуемое время для выполнения спланированных действий и перечень мероприятий, необходимых для достижения поставленной цели.

Классы нарушителей. Исходя из вышеизложенных характеристик, нарушителей можно разделить на группы.

Группа А. Действующие целенаправленно и обладающие практически неограниченным финансовым обеспечением (например, сотрудники иностранной разведки).

Группа Б. Действующие целенаправленно и обладающие ограниченным, но достаточно крупным финансовым обеспечением (например, конкурирующие организации, организованные преступные группы).

Группа В. Действующие целенаправленно, обладающие малым финансовым обеспечением, но имеющие хороший профессиональный уровень подготовки (например, криминальные группы).

Группа Г. Действующие целенаправленно, обладающие малым или вообще отсутствующим финансовым обеспечением и имеющие низкий уровень профессиональной подготовки (например, сотрудники организации).

Группа Д. Действующие не целенаправленно (например, случайные люди).

Таким образом, степень опасности нарушителя в большей степени зависит от его финансового обеспечения, что в конечном итоге позволяет приобретать необходимое техническое обеспечение и подбирать исполнителей с соответствующим уровнем профессиональной подготовки.

Кроме этого, нарушители делятся на внутренних и внешних. Внешний нарушитель находится за пределами информационной системы или объекта при воздействии на них, а внутренний нарушитель – соответственно внутри информационной системы или объекта при воздействии на них.

Способы доступа нарушителя к носителю информации. Для получения доступа к информации нарушитель будет вынужден получить доступ к ее носителю. Для организации мероприятий по контролю доступа к носителю информации необходимо представлять, каким образом нарушитель может получить доступ к нему. Выделяют следующие способы доступа:

1. Физическое проникновение нарушителя (не сотрудник организации) к носителю информации. Такой способ доступа предполагает похищение носителя информации или копирование сведений с носителя информации, к которому нарушитель получил доступ. Способ является широко распространенным ввиду того, что не требует высокой квалификации для его реализации. Таким образом, для противодействия нарушителю и контроля доступа к носителю информации необходимо создать вокруг носителя контролируемую зону.

2. Дистанционное добывание информации без нарушения границ контролируемой зоны. Реализация способа возможна в двух вариантах – в зависимости от формы представления информации. Первый вариант: если форма представления информации – физические поля, тогда нарушитель будет вести перехват информации за счет регистрации соответствующего физического по-

ля (акустическое или электромагнитное). Второй вариант: если информация представлена в электронном виде, то перехват ее возможен из информационной системы за счет несанкционированного доступа к этой информационной системе.

3. Доступ к носителю информации через сотрудника организации, имеющего к нему легальный доступ. Ввиду того что у любого человека есть потребности, а многие из них удовлетворяются за счет использования денежных средств, сотрудник организации, например, за денежное вознаграждение может обеспечить доступ нарушителя к носителю информации и тем самым стать сам нарушителем.

Виды угроз безопасности информации. Доступ нарушителя к носителю информации приводит к реализации угроз безопасности информации. Для того чтобы понять, насколько та или иная угроза является существенной, оценивают ущерб, который причиняется вследствие ее реализации.

Ущерб может быть оценен в денежном эквиваленте (например, когда реализация угрозы разглашения данных платежной карточки приводит к потере денежных средств) или категориально (например, ущерб приемлем или ущерб неприемлем). Если человек принимает полученный ущерб, то это означает, что текущая ситуация, складывающаяся в информационных отношениях, его устраивает.

Когда ущерб в денежном или категориальном исчислении неприемлем, то требуется обеспечить защиту информации, а точнее ее носителя, для минимизации ущерба. Таким образом, необходимость обеспечения безопасности информации обуславливается необходимостью снижения ущерба от ее утраты.

Угрозы по их виду делят на следующие категории:

1) угроза конфиденциальности – нарушение свойства информации быть известной только определенным субъектам информационных отношений (создатель, обладатель информации);

2) угроза целостности – направлена на изменение содержания информации (искажение) или ее уничтожение;

3) угроза доступности – приводит к нарушению доступа к информации, а также влияет на работоспособность ее носителя;

4) угроза подлинности – приводит к невозможности однозначно идентифицировать (определить) автора или источник, откуда она получена;

5) угроза сохранности – ее следствием является невозможность обеспечить такой режим хранения информации, который позволял бы гарантировать ее конфиденциальность, целостность и доступность.

По мере проявления угрозы безопасности информации делятся на преднамеренные и случайные.

Преднамеренные угрозы связаны с целенаправленными действиями человека и носят злонамеренный характер. Именно поэтому нарушителя еще называют злоумышленником, хотя на самом деле злой умысел определяет суд, а до судебного разбирательства действует презумпция невиновности.

Случайные угрозы обусловлены отказом аппаратного обеспечения вследствие нарушения режимов его эксплуатации, отказом программного обеспечения вследствие некорректного взаимодействия с ним человека. Случайные угрозы также обусловлены воздействием внешней среды, а также незлонамеренными действиями человека в силу его некомпетентности, усталости или невнимательности. Эти угрозы могут быть минимизированы за счет повышения культуры пользования аппаратно-программными средствами, обучения людей и получения ими навыков грамотной эксплуатации технических средств обработки информации.

Источники угроз безопасности информации. Источниками угроз безопасности информации являются:

1) человек – вследствие его целенаправленного (преднамеренного) или случайного воздействия на носитель информации;

2) технические средства обработки информации – их некорректная работа (в том числе при некомпетентном обращении с ними) или выход из строя приводит к различным видам угроз;

3) программное обеспечение – ошибки в нем приводят к некорректной его работе и реализации различных видов угроз безопасности информации, а наличие недокументированных возможностей (специально созданных разработчиком программного обеспечения) позволяют посредством их оказывать целенаправленное воздействие;

4) внешняя среда – стихийные бедствия и другие воздействия на носитель информации, в том числе техногенного характера (отключение электропитания и т. д.), являются причиной реализации угроз безопасности информации.

Как было отмечено выше, если ущерб неприемлем, то необходимо информацию защищать.

Различают следующие методы защиты информации:

– правовые – определяют порядок регулирования информационных отношений и требования к средствам и системам защиты информации (нормативные правовые акты Республики Беларусь, приказы по организации и политики безопасности);

– организационные – регламентируют методы и способы достижения требований безопасности (изложенные в нормативных правовых актах) и позволяют повысить эффективность применения средств защиты информации;

– технические – обеспечивают конфиденциальность, целостность и доступность информации за счет использования криптографических и технических средств защиты информации.

Для того чтобы обеспечить безопасность информации, необходимо использовать правовые, организационные и технические методы. Их одновременное применение свидетельствует о том, что безопасность информации обеспечивается **комплексно**.

Следует отметить, что для того чтобы дать однозначный ответ, какие из угроз являются наиболее опасными, необходимо оценить ущерб от их реали-

зации. Это позволит обосновать применение определенных методов и средств защиты информации.

Оценка угроз безопасности информации проводится в целях их идентификации для заданного объекта (носителя информации) и определения степени их влияния на этот объект, что позволяет технически и экономически обосновать систему его защиты.

Оценка угроз безопасности информации должна носить систематический характер. Она проводится с использованием экспертного метода. Такой метод заключается в принятии решения экспертом (специалист в определенной области (в данном случай в области информационной безопасности)) на основании его опыта и знаний. Для снижения влияния субъективных факторов на результат оценки она проводится группой экспертов.

При выполнении оценки угроз безопасности информации необходимо иметь полную информацию об объекте (его назначение, область применения, каким образом он задействован в информационных отношениях). На основании такой информации выполняется непосредственно оценка угроз для заданного объекта.

На **первом этапе** определяют, какие конкретно из угроз безопасности информации для данного объекта могут быть реализованы при доступе к нему нарушителя и к какому виду угроз они относятся.

Рассмотрим пример. Предположим, что текстовая информация, написанная от руки, относящаяся к информации, распространение и (или) предоставление которой ограничено, содержится на бумажном носителе и этот носитель лежит на столе. Существует еще один аналогичный документ, который хранится в сейфе.

В случае физического доступа нарушителя к носителю реализуется угроза конфиденциальности информации, содержащейся на этом носителе, если нарушитель ее прочитает. При физическом доступе к носителю информации также возможна угроза доступности информации, так как нарушитель может уничтожить носитель. В рассматриваемом примере угроза целостности информации не является характерной, так как текст написан от руки и внесение любых изменений в существующий документ будет заметно. Для данного случая угроза подлинности также не является характерной. Вместе с тем, так как угрозы конфиденциальности и доступности возможны, то это приведет также к реализации угрозы сохранности информации.

На **втором этапе** определяют негативные последствия, которые могут наступить вследствие реализации угроз безопасности информации, и оценивают приемлемость ущерба вследствие их наступления.

Вернемся к рассмотренному выше примеру. По результатам первого этапа оценки угроз установлена возможность реализации угроз конфиденциальности и доступности информации для заданного объекта. Негативным последствием реализации угрозы конфиденциальности является разглашение сведений, которые содержатся на рассматриваемом носителе, так как они относятся к инфор-

мации, распространение и (или) предоставление которой ограничено, и поэтому такой ущерб не является приемлемым.

Реализация угрозы доступности приведет к невозможности воспользоваться данным документом, но так как есть еще один, схожий по содержанию, то ущерб от этой угрозы приемлем. Исходя из вышеуказанного, поскольку ущерб от реализации угрозы конфиденциальности неприемлем, то и от реализации угрозы сохранности (см. определение) он также будет неприемлем, и поэтому его нужно минимизировать.

На **третьем этапе** выбирают методы и средства защиты, которые позволят минимизировать ущерб.

Закончим рассмотрение примера. На втором этапе было определено, что ущерб от угроз конфиденциальности и сохранности неприемлем. Так как возникновение угрозы сохранности обусловлено возникновением угрозы конфиденциальности, то, решая проблему конфиденциальности информации, можно решить и проблему ее сохранности. Минимизация ущерба может быть реализована за счет того, что мы ограничим доступ к бумажному носителю информации. Для этого нужно переместить его со стола в более надежное место, например в сейф. В данном случае сейф будет являться средством защиты информации. Метод, который реализуется, – технический, так как сейф – техническое средство.

Как известно, безопасность информации требует комплексного решения проблемы. Поэтому для реализации правовых методов можно предложить разработку инструкции по работе с представленной на бумажных носителях информацией, распространение и (или) предоставление которой ограничено. Эта инструкция будет определять порядок работы с бумажными носителями, для того чтобы минимизировать несанкционированный доступ к ним. В качестве организационных мероприятий необходимо обеспечить регулярную проверку (например, раз в неделю или месяц) выполнения положений этой инструкции.

Утечка информации. Доступ нарушителя к носителю информации приводит к ее утечке, которая, исходя из источников угроз и форм представления информации, делится на три вида:

1. Разглашение информации. В данном случае человек, который является обладателем информации, может неумышленно передать охраняемую законом тайну, например коммерческую, нарушителю. Такая форма утечки приводит к реализации угрозы конфиденциальности информации. Рассмотрим пример. На выставке демонстрируется некоторый товар, и на стенде присутствует его разработчик. Этот человек горд, что его детище демонстрируется на выставке, и охотно отвечает на вопросы посетителей выставки. Одному из посетителей очень понравилась разработка, и он приходит не один день подряд, для того чтобы поговорить о ней с разработчиком. При этом данный посетитель хвалит саму разработку и разработчика. Вот один из сценариев, который при определенных условиях обеспечивает возможность выведывания особенностей данной разработки посетителем. Разработчик в данном случае может и не осо-

знать, что разглашает сведения. Разглашение информации может быть и целенаправленным. Например, человек, который передал сведения, получает за это денежное вознаграждение, что, по сути, его и мотивирует (при определенных потребностях) заниматься такой деятельностью.

2. Утечка информации по техническим каналам. Информация, как отмечалось в разделе 1, представляется в виде физических полей, с помощью которых она передается на расстояние. Один из наиболее значимых видов информации для человека – речевая. При речевой коммуникации происходит передача информации в виде акустических волн через воздушную среду, что, по сути, и создает условия, при которых возможна регистрация речевой информации в виде акустической волны, а в частности – ее перехват. Перехват информации приводит к реализации угрозы конфиденциальности информации.

3. Несанкционированный доступ к информации. Эта форма утечки информации реализуется, например, при доступе нарушителя к сведениям, которые обрабатываются в информационной системе, что также приводит как минимум к реализации угрозы конфиденциальности информации. Необходимо отметить, что для выбранного случая возможна реализация всех видов угроз безопасности информации.

Модель Cyber Kill Chain. Даная модель нарушителя появилась вследствие эволюционного развития крупной корпорации Lokheed Martin (США), которая представила деятельность нарушителя в виде последовательных этапов, на каждом из которых он выполняет определенные действия. Рассмотрим этапы этой модели.

1. Разведка (Reconnaissance). На данном этапе нарушитель собирает информацию об информационной системе доступными для него способами, используя при этом источники общедоступной информации – открытые источники (разведка по открытым источникам – Open Source Intelligence (OSINT)) и программные средства, позволяющие непосредственно взаимодействовать с информационной системой. Полученная информация дает возможность выполнить планирование кибератаки.

2. Вооружение (Weaponization). Нарушитель подготавливает инфраструктуру для совершения кибератаки и программные средства (вредоносные программы) для получения первоначального доступа к информационной системе.

3. Доставка (Delivery). Вредоносная программа определенным образом доставляется в информационную систему. Очень часто для этого используется электронная почта. Такой способ доставки позволяет скомпрометировать множество устройств внутри информационной системы и ускорить процесс достижения нарушителем своей цели.

4. Эксплуатация (Exploitation). Если доставленную, например, по электронной почте в виде прикрепленного файла вредоносную программу запустит на компьютере пользователь, то она, используя уязвимости данного компьютера, установится.

5. Установка (Installation). На данном этапе происходит установка вредоносной программы. Необходимо отметить, что необязательно код вредоносной программы будет запускаться на дисковом накопителе персонального компьютера, запуск может происходить в оперативной памяти компьютера.

6. Получение управления (Command and Control). Запуск вредоносной программы на скомпрометированном компьютере позволяет нарушителю удаленно выполнять на этом компьютере и с его помощью различные действия, используя его вычислительные ресурсы.

7. Действия нарушителя (Actions on Objectives). Нарушитель выполняет необходимые для него действия для достижения цели. Например, у пользователя на компьютере установлено приложение клиент-банк. Нарушитель при определенных условиях может получить доступ к банковскому счету пользователя. Если пользователь кроме логина и пароля для входа в приложение использует многофакторную аутентификацию и одноразовый пароль для входа в приложение приходит к нему на электронную почту, которую он просматривает с этого же компьютера, то нарушитель сможет выполнить перевод денежных средств со счета пользователя.

Рассмотрим еще один пример удаленного использования компьютера пользователя. Нарушитель установит на компьютер пользователя вредоносную программу, которая будет выполнять майнинг криптовалюты. В данном случае для нарушителя этот процесс будет абсолютно выгоден, потому что он будет использовать чужой компьютер и оплачивать счета за электроэнергию ему не надо.

Контрольные вопросы

1. Что называется угрозой безопасности информации?
2. Поясните, в чем необходимость оценки ущерба при реализации угрозы безопасности информации?
3. Какие виды угроз безопасности информации вы знаете? Поясните каждый из видов.
4. Для чего защищают информацию?
5. Зачем оценивают угрозы безопасности информации и как это влияет на безопасность информации?
6. Какие этапы включает в себя алгоритм оценки угроз безопасности информации?
7. Что такое разглашение информации?
8. Что такое утечка информации?
9. Что такое несанкционированный доступ к информации?
10. Какие этапы включает в себя модель Cyber Kill Chain?

4. СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Основная терминология темы [4]. **Информационная безопасность** – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Критически важный объект информатизации – объект информатизации, который на основании критериев отнесения объектов информатизации к критически важным объектам информатизации и показателей уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах включен в Государственный реестр критически важных объектов информатизации.

Национальная безопасность – состояние защищенности национальных интересов Республики Беларусь от внутренних и внешних угроз.

Объект информатизации – средства электронной вычислительной техники вместе с программным обеспечением, в том числе системы управления различного уровня и назначения, информационные системы и сети, автономные стационарные и персональные электронные вычислительные машины, используемые в соответствии с заданной информационной технологией, системы управления информационными, производственными и (или) технологическими процессами.

Система информационной безопасности – совокупность субъектов, обеспечивающих информационную безопасность, которые объединены единым замыслом по защите информационных интересов личности, общества и государства и осуществляют согласованную деятельность в рамках законодательства.

Угроза национальной безопасности – потенциальная или реально существующая возможность нанесения ущерба национальным интересам Республики Беларусь.

Национальные интересы Республики Беларусь. Национальные интересы Республики Беларусь, а соответственно и граждан, которые проживают на этой территории, охватывают все сферы жизни личности общества и государства и изложены в **Концепции национальной безопасности Республики Беларусь**. Они, по своей сути, являются ориентирами ее долгосрочного стабильного развития.

Национальные интересы делятся на стратегические и интересы по сферам жизнедеятельности человека и общества. Стратегические национальные интересы Республики Беларусь следующие:

– независимость, территориальная целостность, суверенитет, незыблемость конституционного строя государства;

– устойчивое экономическое развитие и высокая конкурентоспособность экономики страны;

– достижение высокого уровня и качества жизни граждан.

Необходимо отметить, что все указанные стратегические интересы страны взаимосвязаны друг с другом. Основу любого государства составляют люди, и уровень и качество их жизни обуславливают в принципе существование государства, его территориальную целостность. Если государство необходимо в том виде, в котором оно существует для граждан, значит, граждане будут его беречь и охранять. Безусловно, некоторые граждане переселяются из одной страны в другую, и это вполне нормальный процесс. Внутри государственных границ страны остаются те люди, которых устраивает уровень и качество их жизни. Вместе с тем необходимо заметить, что уровень и качество жизни граждан страны зависят от ее экономики и конкурентоспособности на внешнем рынке.

Национальная безопасность. Сущность национальной безопасности государства заключается в создании таких условий его жизнедеятельности, при которых будет достигаться баланс интересов его граждан, а воздействие внутренних и внешних угроз на национальные интересы минимизируется.

Угрозы национальной безопасности, как внутренние, так внешние, взаимосвязаны друг с другом, и, в целом, характер их воздействия является комплексным. Приведем пример. Отсутствие или нехватка продуктов питания в стране напрямую влияет на качество жизни ее граждан. В случае наступления такого события недоброжелатели могут воспользоваться этой ситуацией, обвинить руководство страны в умышленном создании такой ситуации и поставить вопрос о его легитимности. В данном случае речь идет о комплексе угроз. С одной стороны – желание захватить власть, а с другой – нехватка продуктов питания, которая ставит страну на грань выживания.

Для противодействия внутренним и внешним угрозам необходима система национальной безопасности, которая должна охватывать все сферы жизнедеятельности личности, общества и государства.

Сферы национальной безопасности Республики Беларусь. В национальной безопасности выделяют следующие сферы:

– политическая (включает политические институты, отношения и роль государства в них);

– экономическая (включает отношения, возникающие с производством, распределением и потреблением товаров и услуг);

– научно-технологическая (включает процессы, обеспечивающие научные исследования и разработки, а также подготовку кадров);

– социальная (включает различные аспекты отношений и взаимодействия между людьми и группами людей);

– демографическая (включает процессы воспроизводства населения страны);

– информационная (включает информационные отношения, возникающие между субъектами такой сферы);

– военная (включает процессы, реализация которых позволяет обеспечить мирные условия существования страны);

– экологическая (включает процессы, позволяющие минимизировать антропогенное влияние человека на окружающую среду).

Все указанные сферы критически важны для развития общества и государства, и состояние дел в каждой из них по своей сути определяет возможность достижения национальных интересов.

Информационная безопасность. Данная сфера позволяет обеспечить баланс интересов участников информационных отношений и соблюдение норм права, регулирующего эти отношения, что в совокупности позволяет достичь национальных интересов в информационной сфере. Основу деятельности в сфере информационной безопасности составляет целенаправленное противодействие внешним и внутренним угрозам в информационной сфере.

Национальные интересы Республики Беларусь в информационной сфере. К национальным интересам Республики Беларусь в информационной сфере относятся:

– реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;

– формирование и поступательное развитие информационного общества;

– равноправное участие Республики Беларусь в мировых информационных отношениях;

– преобразование информационной индустрии в экспортно ориентированный сектор экономики;

– эффективное информационное обеспечение государственной политики;

– обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

Рассмотрим вышеуказанные национальные интересы Республики Беларусь в информационной сфере. У каждого гражданина страны есть право на информацию, причем не только на ее получение, но и на распространение. Причем распространение достоверных, а не ложных сведений, поскольку, как мы ранее замечали, они будут влиять на принятие решений.

Развитие информационного общества является важнейшим приоритетом, но оно невозможно без знаний в области информационной безопасности. Это связано с тем, что очень часто различные информационные ресурсы создаются для обеспечения влияния на мнение и решения людей путем предоставления недостоверных или неполных сведений.

Участие Республики Беларусь в мировых информационных отношениях способствует развитию ее экономического потенциала, выходу на рынки иностранных государств и взаимовыгодному сотрудничеству (гуманитарное сотрудничество, развитие науки и техники, культуры).

Современные производства для обеспечения стабильного и гарантированного качества выпускаемой ими продукции используют информационные и автоматизированные системы, что позволяет рассматривать в некоторой степени преобразование информационной индустрии в экспортно ориентированный сектор экономики. Недостаточность информационного обеспечения государственной политики приводит к принятию неверных решений, перерасходу ресурсов, что в конечном итоге влияет на экономику страны. Применение раз-

личных информационных систем, обеспечивающих поддержку и принятие решений, является важной для государства задачей.

Резюмируя вышеуказанное, необходимо отметить, что те информационные и автоматизированные системы, которые существенно влияют на развитие страны, требуют пристального внимания, касающегося обеспечения их надежного и устойчивого функционирования при различных видах воздействий.

Угрозы информационной безопасности Республики Беларусь. Рассмотрим примеры угроз информационной безопасности:

– деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам – открытость информационного пространства Республики Беларусь обуславливает возникновение такой угрозы. В настоящее время существует немало информационных ресурсов, планомерно и целенаправленно воздействующих на граждан страны;

– нарушение функционирования критически важных объектов информатизации – ввиду того что такие объекты непосредственно влияют на процессы обеспечения качества жизни граждан, то надежность их функционирования при различных видах воздействий является важнейшей задачей;

– утрата либо разглашение сведений, составляющих охраняемую законодательством тайну и способных причинить ущерб национальной безопасности. Необходимо отметить, что в зависимости от утраченных сведений ущерб может быть причинен всем вышеуказанным сферам жизнедеятельности человека, а соответственно, и стратегическим национальным интересам страны и граждан, проживающих в ней.

Критически важный объект информатизации. Критически важный объект информатизации в своем составе содержит технические, программные, программно-аппаратные средства (в том числе средства защиты информации), обрабатываемую информацию, системы управления информационными, производственными и (или) технологическими процессами.

Существуют четыре группы критериев, которые позволяют отнести объект информатизации к критически важному объекту.

1. Социальная значимость объекта информатизации. Это объекты, которые обеспечивают жизнедеятельность человека. Сюда относятся объекты информатизации жилищно-коммунального хозяйства, здравоохранения, учреждений образования и т. п.

2. Экономическая значимость объекта информатизации. Такие объекты обеспечивают функционирование основных отраслей экономики, которые проводят безналичные и межбанковские расчеты, осуществляют процессинг.

3. Экологическая значимость объекта информатизации. Реализация угроз на таких объектах приводит к ущербу окружающей среды.

4. Информационная значимость объекта информатизации. Объекты, которые используются в области связи и средств массовой информации.

Структура и функции системы национальной безопасности Республики Беларусь. Основными функциями системы информационной безопасности Республики Беларусь являются:

– оценка состояния информационной безопасности в государстве, выявление источников угроз, определение приоритетных направлений их предотвращения и нейтрализации, а также противодействия им;

– координация деятельности органов государственной власти и других органов, решающих задачи обеспечения информационной безопасности Республики Беларусь;

– проведение единой технической политики в области информационной безопасности Республики Беларусь;

– обеспечение контроля создания и использования средств защиты информации посредством обязательного лицензирования деятельности в области защиты информации, сертификации и экспертизы продукции информационных технологий и аттестации объектов информатизации по требованиям безопасности информации;

– совершенствование и развитие единой системы подготовки кадров в области информационной безопасности Республики Беларусь.

Рассмотрим обобщенную структуру системы информационной безопасности Республики Беларусь (рис. 4.1).

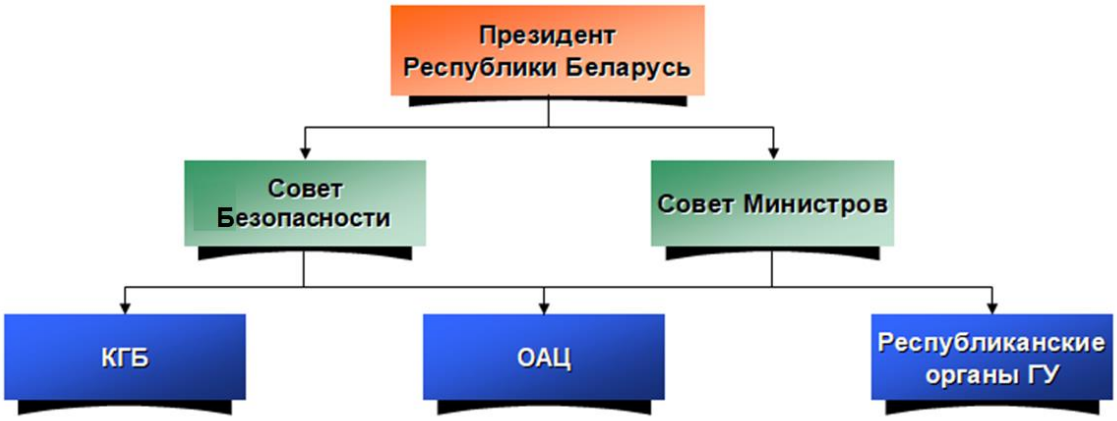


Рис. 4.1. Обобщенная структура системы информационной безопасности Республики Беларусь

Президент Республики Беларусь – реализует свои полномочия через Совет Безопасности и Совет Министров, санкционирует действия по обеспечению информационной безопасности, в соответствии с законодательством формирует, реорганизует и упраздняет подчиненные ему органы и силы обеспечения информационной безопасности.

Комитет государственной безопасности (КГБ) – обеспечивает разработку системы мер по защите государственных секретов, а также обеспечивает государственные органы и иные организации правительственной и оперативной

связью и осуществляет контроль и лицензирование деятельности субъектов в рамках своих компетенций и в соответствии с законодательством.

Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ) – обеспечивает разработку системы мер по обеспечению безопасности информации при использовании информационных сетей, систем и ресурсов национального сегмента сети Интернет, а также осуществляет контроль и лицензирование деятельности субъектов в рамках своих компетенций и в соответствии с законодательством.

Республиканские органы государственного управления – решают задачи обеспечения безопасности информации в соответствии с законодательством и в пределах своих компетенций.

Субъекты хозяйствования Республики Беларусь, выполняющие работы на основании лицензий. Лицензия представляет собой специальное разрешение на выполнение некоторых действий, указанных в ней.

Субъектами хозяйствования осуществляется деятельность в области защиты информации при условии наличия лицензии на соответствующий вид деятельности. Такими субъектами являются следующие категории организаций:

– научно-исследовательские, проектные и конструкторские организации;

– сертификационные и испытательные центры (лаборатории);

– предприятия, учреждения и иные организации различных форм собственности.

Деятельность субъектов хозяйствования Республики Беларусь в ходе проведения ими научно-исследовательских, проектных и опытно-конструкторских работ в сфере защиты информации координирует научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации» (НИИ ТЗИ).

Контрольные вопросы

1. Что называется угрозой безопасности информации?
2. Поясните, в чем необходимость оценки ущерба при реализации угрозы безопасности информации?
3. Какие виды угроз безопасности информации вы знаете? Поясните каждый из видов.
4. Для чего защищают информацию?
5. Зачем оценивают угрозы безопасности информации и как это влияет на безопасность информации?
6. Что относится к угрозам информационной безопасности Республики Беларусь?
7. Что такое критически важный объект информатизации?
8. На основании каких критериев объект информатизации относят к критически важному?
9. Перечислите основные функции системы информационной безопасности Республики Беларусь.
10. Какие субъекты входят в структуру системы информационной безопасности Республики Беларусь?

5. МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Основная терминология темы [1, 5]. **Защита информации** – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Несанкционированное воздействие на информацию – изменение или уничтожение информации, осуществляемое с нарушением установленных прав или правил.

Несанкционированный доступ к информации – доступ к информации, осуществляемый с нарушением установленных прав или правил разграничения доступа.

Средства криптографической защиты информации – программные, программно-аппаратные средства, реализующие один или несколько криптографических алгоритмов (шифрование, выработка и проверка электронной цифровой подписи, хеширование, имитозащита) и криптографические протоколы, а также функции управления криптографическими ключами и функциональные возможности безопасности.

Средства технической защиты информации – технические, программные, программно-аппаратные средства, предназначенные для защиты информации от несанкционированного доступа и несанкционированных воздействий на нее, блокирования правомерного доступа к ней, иных неправомерных воздействий на информацию, а также для контроля ее защищенности.

Направления обеспечения безопасности информации. Под безопасностью информации следует понимать состояние ее защищенности от угроз и рисков. По сути, безопасность информации – это следствие реализации мер по защите информации. Согласно Положению о технической и криптографической защите информации, утвержденному Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 (в редакции Указа Президента Республики Беларусь от 09.12.2019 № 449), можно условно выделить два направления по защите информации:

– техническая защита информации;

– криптографическая защита информации.

Согласно вышеуказанному Положению техническая защита информации – это деятельность, направленная на обеспечение конфиденциальности, целостности, доступности и сохранности информации техническими мерами без применения средств криптографической защиты информации. Криптографическая защита информации – деятельность, направленная на обеспечение конфиденциальности, контроля целостности и подлинности информации с использованием средств криптографической защиты информации.

Исходя из вышеизложенного, можно выделить два направления обеспечения безопасности информации.

Классификация методов защиты информации. Исходя из определения термина «защита информации», представленного в Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите ин-

формации» (см. пункт «Основная терминология» настоящего раздела), можно выделить следующие виды методов защиты информации:

– правовые;

– организационные;

– технические.

Следует отметить, что перечисленные методы используются для реализации одноименных мер по защите информации, представленных в определении термина «защита информации». Термины «мера» (т. е. мероприятие) и «метод» не являются синонимичными. Под мерой (т. е. мероприятием) следует понимать совокупность действий, направленных на осуществление чего-либо. Очевидно, что под мерой по защите информации следует понимать совокупность действий, направленных на осуществление защиты информации. Под методом следует понимать способ осуществления чего-либо. Соответственно, под методом защиты информации следует понимать способ осуществления мер по защите информации.

Правовые методы по защите информации основаны на использовании требований, изложенных в нормативных правовых актах в сфере защиты информации. По сути, эти методы направлены на регламентацию действий по защите информации в стране.

Организационные методы по защите информации состоят:

– в разработке на предприятии локальных документов в сфере защиты информации (политик, регламентов, инструкций, распоряжений руководителя и т. п.) с учетом требований, изложенных в вышеуказанных нормативных правовых актах;

– создании условий для выполнения требований, изложенных в вышеуказанных локальных документах.

Технические методы по защите информации основаны на использовании средств технической и криптографической защиты информации (см. пункт «Основная терминология темы» настоящего раздела). Одной из разновидностей средств технической защиты информации являются средства, используемые для обеспечения защиты информации от утечки по техническим каналам.

Средства технической защиты информации от утечки по техническим каналам. Выделяют следующие виды технических каналов утечки информации (более подробно об этих каналах – в разделе 9 «Защита информации от технической разведки»):

– визуально-оптический;

– канал побочного электромагнитного излучения и наводок;

– акустический.

Средства технической защиты информации от утечки по техническим каналам условно делятся на две группы:

1) пассивные;

2) активные.

Эти средства различаются не только составом, но и принципом функционирования. Принцип функционирования пассивных технических средств защи-

ты информации от утечки по техническим каналам может быть описан с помощью следующего выражения: $\downarrow \frac{\downarrow P_{\text{с}}}{P_{\text{ш}}}$. Выражение для описания принципа функционирования активных технических средств защиты информации от утечки по техническим каналам выглядит следующим образом: $\downarrow \frac{P_{\text{с}}}{\uparrow P_{\text{ш}}}$.

В обоих выражениях с помощью стрелок, направленных вниз и вверх, обозначены соответственно процессы снижения и увеличения, с помощью буквосочетания $P_{\text{с}}$ – интенсивность (напряженность) информационного сигнала, формируемого источником информации, распространение и (или) предоставление которой ограничено, а с помощью буквосочетания $P_{\text{ш}}$ – интенсивность (напряженность) шума в среде, по которой эта информация распространяется.

Таким образом:

1) принцип функционирования пассивных технических средств защиты информации от утечки по техническим каналам основан на снижении отношения сигнал/шум в среде, по которой информация распространяется путем снижения интенсивности (напряженности) информационного сигнала, формируемого источником этой информации;

2) принцип функционирования активных технических средств защиты информации от утечки по техническим каналам основан на снижении отношения сигнал/шум в среде, по которой информация распространяется путем увеличения интенсивности (напряженности) циркулирующих в ней шумов.

В табл. 5.1–5.3 представлены наименования и примеры пассивных и активных технических средств защиты информации от утечки по каждому из технических каналов.

Таблица 5.1

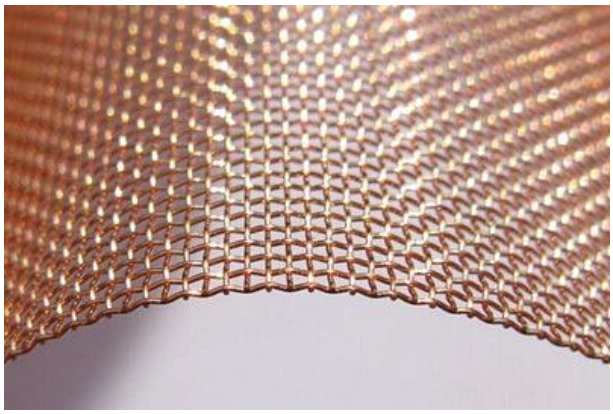
Технические средства защиты информации
от утечки по визуально-оптическому каналу

Пассивные технические средства для защиты информации от утечки по техническому каналу	Активные технические средства для защиты информации от утечки по техническому каналу
Материалы для маскирования объектов в видимом и инфракрасном диапазонах длин волн 	Дымовые «завесы» 

Таблица 5.2

Технические средства защиты информации
от утечки по каналу побочного электромагнитного излучения

Пассивные технические средства для защиты информации от утечки по техническому каналу	Активные технические средства для защиты информации от утечки по техническому каналу
Экранирующие и радиопоглощающие материалы, используемые для создания экранированных помещений или средств обработки информации в защищенном исполнении	Устройства пространственного и линейного электромагнитного зашумления



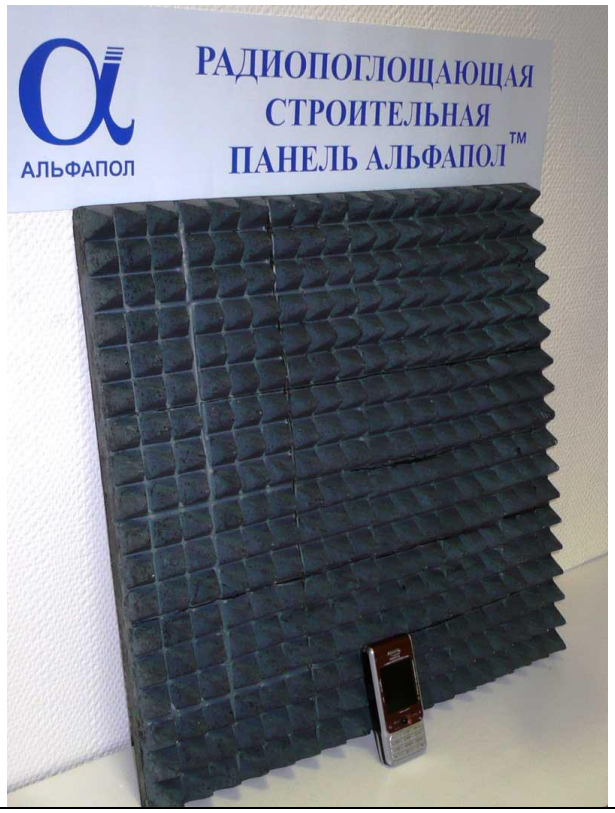


Таблица 5.3

Технические средства защиты информации
от утечки по акустическому каналу

Пассивные технические средства для защиты информации от утечки по техническому каналу	Активные технические средства для защиты информации от утечки по техническому каналу
Звукоизолирующие и звукопоглощающие материалы  	Генераторы акустического шума 

Процесс внедрения и использования технических средств защиты информации от утечки по техническим каналам должен включать в себя процедуру оценки их эффективности. Данная процедура основана на использовании специальных технических средств, которое регламентировано следующими документами:

– Положение о ввозе на таможенную территорию Евразийского экономического союза и вывозе с таможенной территории Евразийского экономического союза специальных технических средств, предназначенных для негласного получения информации (Приложение № 16 к Решению Коллегии Евразийской экономической комиссии от 21 апреля 2015 г. № 30);

– постановление Совета Министров Республики Беларусь от 1 августа 2012 г. № 722 «О некоторых вопросах проведения экспертизы образцов специальных технических средств, предназначенных для негласного получения информации».

Указанные два документа по сути содержат перечень мероприятий, который относится к правовым методам защиты информации от утечки по техническим каналам.

Контрольные вопросы

1. В чем разница между несанкционированным доступом к информации и несанкционированным воздействием на нее?
2. Что такое средство технической защиты информации?
3. Что такое средство криптографической защиты информации?
4. Какие направления обеспечения безопасности информации можно выделить?
5. В чем разница между выделяемыми направлениями обеспечения безопасности информации?
6. Какие методы защиты информации можно выделить?
7. Какие выделяют виды технических каналов утечки информации?
8. На какие группы делятся средства технической защиты информации от утечки по техническим каналам? В чем различия между средствами каждой из групп?
9. Приведите примеры пассивных средств технической защиты информации от утечки по техническим каналам.
10. Приведите примеры активных средств технической защиты информации от утечки по техническим каналам.

6. СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Основная терминология темы [1, 5]. **Защита информации** – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах.

Информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств.

Информационная технология – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации.

Система защиты информации – совокупность мер по защите информации, реализованных в информационной системе.

Проектирование системы защиты информации. В Республике Беларусь процессы проектирования и создания системы защиты информации (СЗИ) регламентируются Положением о порядке технической и криптографической защиты информации в информационных системах (ИС), предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» с изменениями и дополнениями, внесенными приказами Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195 и от 29 декабря 2022 г. № 210 (далее по тексту раздела – Положение) [6].

В соответствии с п. 3 Положения проектирование и создание СЗИ являются составляющими комплекса мероприятий по технической и криптографической защите информации в ИС. Полный перечень этих мероприятий следующий:

1) проектирование СЗИ;

2) создание СЗИ;

3) аттестация СЗИ;

4) обеспечение функционирования СЗИ;

5) обеспечение защиты информации в случае прекращения эксплуатации ИС.

По сути, представленный перечень можно условно назвать «жизненным циклом» СЗИ. Он начинается с момента инициирования процедуры проектирования этой системы и заканчивается в момент прекращения эксплуатации ИС, в составе которой она функционировала.

Рассмотрим особенности и порядок реализации мероприятий по проектированию СЗИ. Согласно п. 7 Положения перед проектированием СЗИ необходимо выполнить следующие действия:

1) категорирование (по сути, классификация) информации, которая обрабатывается или будет обрабатываться в ИС, для которой создается СЗИ;

2) классификация ИС на основе следующих признаков:

– принадлежность ИС;

– категория (вид) информации, обрабатываемой в ИС;

– взаимодействие ИС с открытыми каналами передачи данных.

В ходе реализации первого из перечисленных действий необходимо руководствоваться законами Республики Беларусь в области информации, информатизации и защиты информации. Эти законы, а также сведения о категориях и типах информации представлены в разделе 2 «Информация ограниченного распространения и ее демаскирующие признаки» учебного пособия.

В ходе реализации второго из перечисленных действий необходимо принять решение о том, к какому классу отнести ИС, для которой создается СЗИ. Для этого необходимо ответить на следующие вопросы:

1) ИС является государственной или негосударственной?

2) В ИС обрабатывается общедоступная информация или информация, распространение и (или) предоставление которой ограничено?

3) Если в ИС обрабатывается информация, распространение и (или) предоставление которой ограничено, то к какому(-им) виду(-ам) относится эта информация:

– персональные данные, за исключением специальных персональных данных;

– специальные персональные данные, за исключением биометрических и генетических персональных данных;

– биометрические и генетические персональные данные;

– коммерческая тайна;

– служебная информация ограниченного распространения?

4) Подключена ли ИС к открытым (т. е. не выделенным физически) каналам передачи данных?

Сведения о классах ИС, основанные на ответах на перечисленные вопросы, представлены в табл. 6.1.

Таблица 6.1

Сведения о классах ИС

<table>
<tr><th>Класс ИС</th><th>Принадлежность ИС</th><th>Категория (вид) информации, обрабатываемой в ИС</th><th>Наличие подключения к открытым каналам передачи данных</th></tr>
<tr><td>6-частн</td><td>Государственная</td><td rowspan="4">Общедоступная</td><td rowspan="2">Нет</td></tr>
<tr><td>6-гос</td><td>Негосударственная</td></tr>
<tr><td>5-частн</td><td>Государственная</td><td rowspan="2">Да</td></tr>
<tr><td>5-гос</td><td>Негосударственная</td></tr>
<tr><td>4-ин (3-ин)</td><td rowspan="5">–</td><td>Персональные данные, за исключением специальных персональных данных</td><td rowspan="5">Нет (Да)</td></tr>
<tr><td>4-спец (3-спец)</td><td>Специальные персональные данные, за исключением биометрических и генетических персональных данных</td></tr>
<tr><td>4-бг (3-бг)</td><td>Биометрические и генетические персональные данные</td></tr>
<tr><td>4-юл (3-юл)</td><td>Коммерческая тайна</td></tr>
<tr><td>4-дсп (3-дсп)</td><td>Служебная информация ограниченного распространения</td></tr>
</table>

По результатам выполнения действий, предшествующих этапу проектирования СЗИ, необходимо составить акт отнесения ИС к классу типовых ИС. Форма этого акта представлена на рис. 6.1. Эта форма приведена в Приложении 2 Положения.

УТВЕРЖДАЮ

_____

(наименование должности

_____

руководителя организации)

_____

(подпись, инициалы, фамилия)

___.__.20___

АКТ
отнесения информационной системы к классу
типовых информационных систем

_____

(наименование и место нахождения организации,

_____

полное наименование информационной системы)

Настоящий акт составлен комиссией, назначенной приказом от ___ _____ 20__ г. № _____, в составе:

председателя _____,

членов комиссии: _____

о том, что информационной системе _____,

(полное наименование информационной системы)

в которой обрабатывается _____

(указывается наименование

_____ и которая

или конкретные виды информации и категория доступа к ней)

_____ к открытым каналам передачи данных,

подключена (не подключена)

присвоен класс _____

Председатель комиссии _____ _____

(подпись) (инициалы, фамилия)

Члены комиссии: _____ _____

(подпись) (инициалы, фамилия)

_____ _____

(подпись) (инициалы, фамилия)

Рис. 6.1. Форма акта отнесения ИС к классу типовых ИС

Согласно п. 8 Положения на этапе проектирования СЗИ должны быть выполнены следующие действия:

1) анализ структуры ИС и информационных потоков;
2) издание политики информационной безопасности;
3) определение требований к СЗИ в техническом задании на создание СЗИ;
4) выбор средств технической и криптографической защиты информации;
5) разработка (корректировка) общей схемы СЗИ.

Перед проведением ***первого действия*** в рамках этапа проектирования СЗИ, т. е. анализа структуры ИС и информационных потоков, представляется целесообразным выполнить классификацию активов этой системы, так как, согласно Положению, цель такого анализа – это:

– определение количества, состава и мест размещения программно-технических средств ИС;

– определение физических и логических границ ИС.

К активам ИС относятся:

– средства вычислительной техники;

– телекоммуникационное оборудование, системное и прикладное программное обеспечение;

– информационные ресурсы, входящие в состав ИС.

В ходе реализации ***второго действия*** в рамках этапа проектирования СЗИ, т. е. в ходе издания политики информационной безопасности, необходимо учитывать требования, предъявляемые к содержанию этого локального документа. Эти требования представлены в п. 9 Положения. Согласно обозначенному пункту в политике информационной безопасности должны быть отражены:

– цели и принципы защиты информации;

– перечень ИС, отнесенных к классам типовых ИС;

– сведения о подразделении (должностном лице), ответственном за обеспечение защиты информации;

– обязанности пользователей ИС;

– порядок взаимодействия ИС с другими ИС.

Ниже представлены некоторые рекомендации по составлению политики информационной безопасности в соответствии с вышеперечисленными требованиями.

В качестве ***цели защиты информации*** в политике информационной безопасности, издаваемой в рамках проектирования СЗИ, можно определить следующую: поддержание свойств конфиденциальности, целостности, доступности, подлинности и сохранности информации, обрабатываемой в ИС. Эта цель коррелирует с определением термина «политика информационной безопасности», приведенном в Положении.

В качестве ***принципов защиты информации*** в политике информационной безопасности, издаваемой в рамках проектирования СЗИ, целесообразно определить следующие:

– законность;

– комплексность;

– непрерывность;

– минимизация полномочий;

– персональная ответственность;

– контроль.

Следует отметить, что реализуемые в организации меры по защите информации соответствуют принципу законности в том случае, если они не противоречат требованиям национальных технических, нормативных и правовых актов в сфере защиты информации.

Обсуждаемые меры соответствуют принципу комплексности в том случае, если являются мерами разного характера, т. е. представляют собой комплекс организационных, правовых и технических мер.

В соответствии с принципом минимизации полномочий работникам организации необходимо предоставлять доступ к активам информационной системы ровно в той степени, в которой это им нужно для того, чтобы выполнять свои должностные обязанности.

Согласно принципу персональной ответственности каждый работник организации должен нести персональную ответственность за те свои действия, которые приводят к нарушению требований по защите информации.

Принцип контроля в ходе реализации мер по защите информации соблюдается в случае, когда в организации назначено лицо, ответственное за мониторинг соблюдения этих мер.

В перечне ИС, отнесенных к классам типовых ИС, который приводится в политике информационной безопасности, должны фигурировать те же наименования и классы ИС, что фигурируют в актах отнесения ИС к классу типовых ИС, составленных в ходе выполнения действий, предшествующих этапу проектирования СЗИ.

При описании в политике информационной безопасности ***порядка взаимодействия ИС с другими ИС*** необходимо учитывать данные, которые представлены в Приложении 4 Положения (рис. 6.2).

	6-частн/6-гос	5-частн/5-гос	4-ин/4-спец/4-бг/4-юл/4-дсп	3-ин/3-спец/3-бг/3-юл/3-дсп
4-ин	х	не допускается	х	не допускается
4-спец	х	не допускается	х	не допускается
4-бг	х	не допускается	х	не допускается
4-юл	х	не допускается	х	не допускается
4-дсп	х	не допускается	х	не допускается
3-ин	не допускается	х/о	не допускается	х/о
3-спец	не допускается	х/о	не допускается	х/о
3-бг	не допускается	х/о	не допускается	х/о
3-юл	не допускается	х/о	не допускается	х/о
3-дсп	не допускается	х/о	не допускается	х/о

х – физически выделенный канал передачи данных;
о – наличие подключения к открытым каналам передачи данных (в том числе к глобальной информационной сети Интернет)

Рис. 6.2. Требования к организации взаимодействия ИС, представленные в Приложении 4 Положения

В ходе реализации ***третьего действия*** в рамках этапа проектирования СЗИ, т. е. в ходе определения требований к СЗИ в техническом задании на создание СЗИ, необходимо учитывать требования, предъявляемые к содержанию этого документа. Эти требования приведены в п. 10 Положения. Ключевыми составляющими технического задания на создание СЗИ в соответствии с этими требованиями являются следующие сведения:

– наименование ИС с указанием присвоенного ей класса типовых ИС;
– требования к СЗИ;
– сведения об организации взаимодействия ИС с иными ИС;
– порядок обезличивания персональных данных (в случае их обработки в ИС);
– требования к средствам криптографической защиты информации;

– перечень документации на СЗИ.

Ниже представлены некоторые рекомендации по составлению технического задания на СЗИ.

Наименования ИС и их классов, которые приводятся в техническом задании на создание СЗИ, должны совпадать с соответствующими наименованиями и классами, представленными в актах отнесения ИС к классу типовых ИС, составленных в ходе выполнения действий, предшествующих этапу проектирования СЗИ.

Требования к СЗИ определяются в техническом задании на создание СЗИ в соответствии с Приложением 3 Положения, в котором приведен перечень обязательных и рекомендуемых для выполнения требований к СЗИ для информационных систем 4-го и 3-го классов. Эти требования разделены на следующие группы:

1) аудит безопасности;

2) требования к обеспечению защиты данных;

3) требования по обеспечению идентификации и аутентификации;

4) требования по защите СЗИ ИС;

5) обеспечение криптографической защиты информации;

6) дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре;

7) иные требования

Сведения об организации взаимодействия ИС с иными ИС, приводимые в техническом задании на создание СЗИ, должны коррелировать с данными, которые представлены в Приложении 4 Положения (см. рис. 6.2).

При изложении ***порядка обезличивания персональных данных*** в техническом задании на создание СЗИ необходимо учитывать, что в соответствии с Приложением 5 Положения выделяют следующие методы обезличивания персональных данных:

– введение идентификаторов (замена персональных данных или части персональных данных, позволяющих идентифицировать их субъекта, идентификаторами);

– изменение состава (обобщение, изменение или удаление атрибутов персональных данных, позволяющих идентифицировать их субъекта);

– декомпозиция (разбиение множества атрибутов персональных данных на подмножества);

– перестановка (взаимное перемещение атрибутов персональных данных);

– зашифрование (применение средств криптографической защиты информации).

При представлении в техническом задании на создание СЗИ ***перечня документации на СЗИ*** необходимо учитывать, что эта документация должна содержать сведения:

– о способах разграничения доступа пользователей к объектам ИС;

– порядке резервирования и уничтожения информации;

– порядке защиты от вредоносного программного обеспечения;

– порядке использования съемных носителей информации;

– порядке использования электронной почты;

– порядке обновления средств защиты информации;

– порядке осуществления контроля (мониторинга) за функционированием ИС и СЗИ;

– порядке реагирования на события информационной безопасности и ликвидации их последствий;

– порядке управления криптографическими ключами (т. е. порядке генерирования, распределения, хранения таких ключей, предоставления доступа к ним и их уничтожения).

По сути, документация на СЗИ может представлять собой совокупность таких локальных документов, как Инструкция о порядке разграничения доступа пользователей к объектам ИС, Инструкция о порядке защиты от вредоносного программного обеспечения, Инструкция о порядке использования съемных носителей информации и т. п., или может быть включена в качестве разделов в политику информационной безопасности организации.

В ходе реализации ***четвертого действия*** в рамках этапа проектирования СЗИ необходимо осуществить выбор средств технической и криптографической защиты информации, с помощью которых можно обеспечить выполнение требований к СЗИ, определенных в техническом задании на эту систему. Следует отметить, что эти средства должны быть выбраны из числа средств технической и криптографической защиты информации, имеющих сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам государственной экспертизы, проводимой Оперативно-аналитическим центром при Президенте Республики Беларусь. Перечень таких средств представлен на сайте указанного центра.

И наконец, в ходе реализации ***пятого действия*** в рамках этапа проектирования СЗИ, т. е. в ходе разработки или корректировки общей схемы СЗИ, необходимо, как было отмечено выше, учитывать результаты реализации первого действия, а также требования к содержанию общей схемы СЗИ, изложенные в п. 11 Положения. Согласно обозначенному пункту общая схема СЗИ должна содержать:

– наименование ИС;

– класс типовых ИС;

– места размещения объектов ИС;

– сведения о физических границах ИС;

– сведения о внешних и внутренних информационных потоках и протоколах обмена защищаемой информацией.

Подчеркнем, что в общей схеме СЗИ должны фигурировать те же наименования и классы ИС, что и в политике информационной безопасности, техническом задании на создание СЗИ и актах отнесения ИС к классу типовых ИС, составленных в ходе выполнения действий, предшествующих этапу проектирования СЗИ.

Таким образом, по результатам выполнения действий, предшествующих этапу проектирования СЗИ, а также по результатам выполнения действий в рамках этого этапа должны быть разработаны следующие документы:

– акт отнесения ИС к классу типовых ИС;

– политика информационной безопасности;

– техническое задание на создание СЗИ;

– общая схема СЗИ.

Создание СЗИ. Следующим после проектирования этапом «жизненного цикла» СЗИ является этап создания СЗИ. Согласно п. 15 Положения на этом этапе должны быть выполнены следующие действия:

1) внедрение средств технической и криптографической защиты информации, проверка их работоспособности и совместимости с другими объектами информационной системы;

2) разработка (корректировка) документации на СЗИ по перечню, определенному в техническом задании;

3) реализация организационных мер по защите информации.

Согласно п. 15 Положения в ходе выполнения ***первого действия*** в рамках этапа создания СЗИ должно быть реализовано следующее:

– монтаж и наладка средств технической и криптографической защиты информации;

– смена установленных по умолчанию реквизитов доступа к средствам технической и криптографической защиты информации;

– проверка корректности выполнения требований безопасности средствами технической и криптографической защиты информации.

При успешной реализации вышеперечисленного можно приступать к выполнению ***второго действия*** в рамках этапа создания СЗИ. Это действие состоит в разработке или корректировке документации на СЗИ с учетом соответствующего перечня, приведенного в техническом задании на создание СЗИ. Представляется целесообразным обеспечить корреляцию требований, излагаемых в этой документации, с требованиями к СЗИ, также приведенными в указанном задании. В табл. 6.2 представлены сведения, подлежащие представлению в документации на СЗИ, в соответствии с группами требований к СЗИ ИС.

Таблица 6.2

Сведения, подлежащие представлению в документации на СЗИ, в соответствии с группами требований к СЗИ ИС

Сведения, подлежащие представлению в документации на СЗИ	Наименования групп требований к СЗИ ИС
Описание способов разграничения доступа пользователей к объектам ИС	Требования по обеспечению идентификации и аутентификации. Требования по защите СЗИ ИС
Сведения о порядке резервирования и уничтожения информации	Требования к обеспечению защиты данных. Дополнительные требования по обеспечению защиты информации виртуальной инфраструктуры. Иные требования
Сведения о порядке защиты от вредоносного программного обеспечения	Иные требования
Сведения о порядке использования съемных носителей информации	Требования по обеспечению защиты данных
Сведения о порядке использования электронной почты	Иные требования
Сведения о порядке обновления СЗИ	Требования по защите СЗИ ИС
Сведения о порядке осуществления контроля (мониторинга) за функционированием ИС и СЗИ	Аудит безопасности. Требования по обеспечению защиты данных. Иные требования
Сведения о порядке реагирования на события информационной безопасности и ликвидации их последствий	Иные требования
Сведения о порядке управления криптографическими ключами	Обеспечение криптографической защиты информации

По завершении разработки или корректировки документации на СЗИ необходимо выполнить ***третье, заключительное, действие*** в рамках этапа создания СЗИ. Как было отмечено выше, это действие подразумевает реализацию организационных мер по защите информации. В соответствии с п. 19 Положения цель реализации таких мер состоит в создании условий для выполнения требований, изложенных в документации на СЗИ. В начале процесса реализации этих мер необходимо довести до сведения пользователей ИС под подпись

эти требования. В ходе процесса реализации этих мер представляется важным проводить контроль за их соблюдением, а также организовывать обучение пользователей ИС. Следует отметить, что контроль и обучение являются составляющими перечня действий, которые должны быть реализованы в рамках такого этапа «жизненного цикла» СЗИ, как эксплуатация.

Контрольные вопросы

1. Что такое система защиты информации?
2. Какой документ регламентирует процессы проектирования и создания системы защиты информации?
3. Какие действия должны быть выполнены на этапе проектирования системы защиты информации?
4. Какие сведения должны быть отражены в политике информационной безопасности?
5. Какие сведения должны быть отражены в техническом задании на создание системы защиты информации?
6. Какие выделяют методы обезличивания персональных данных?
7. Какие сведения должны быть отражены в общей схеме системы защиты информации?
8. Какие документы должны быть разработаны по результатам реализации этапа проектирования системы защиты информации?
9. Какие действия должны быть выполнены на этапе создания системы защиты информации?
10. Какова цель реализации организационных мер при создании и эксплуатации системы защиты информации?

7. ФИЗИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ

Основная терминология темы. **Дверь** – устройство, состоящее из дверной коробки и подвижно закрепленного дверного полотна (или полотен), которое в закрытом положении фиксируется в дверной коробке замком, запирающим устройством или засовом, предназначенное для открывания и закрывания проема или прохода.

Жалюзи – инженерно-технические средства защиты, представляющие собой решетчатые ставни из параллельно расположенных подвижных (перемещающихся вдоль направляющих и (или) поворачивающихся около продольной оси) полосообразных элементов (пластин), предназначенные для перекрытия и защиты проема ограждающей конструкции.

Замковое устройство – устройство, обеспечивающее секретность отпирания двери, а также управляющее действием запирающего механизма или блокирующее движение его силовых элементов.

Защитное остекление – остекление, выполненное на основе высокопрочного стекла.

Инженерно-технические средства защиты – средства, применяемые для обеспечения необходимого противодействия несанкционированному проникновению на охраняемые объекты, взлому и другим преступным действиям. К инженерно-техническим средствам защиты относятся решетки, ставни, противовзломные и пуленепробиваемые двери, окна, роллеты, жалюзи, защитное остекление и т. п.

Контролируемая зона – территория объекта, на которой исключается неконтролируемое пребывание людей или транспортных средств без постоянного или разового доступа.

Нарушитель – лицо, пытающееся проникнуть или проникшее на охраняемый объект без разрешения ответственного лица, пользователя, владельца или жильца.

Объект – здания, сооружения, строения, их части строительных конструкций (включая изолированные помещения), иные объекты недвижимого имущества, участки местности, транспортные средства и другое имущество, подлежащее охране.

Решетка – инженерно-техническое средство защиты, представляющее собой не сплошную конструкцию из взаимно переплетенных и скрепленных между собой прутьев, полос или профилей и предназначенное для защиты проемов в ограждающей конструкции.

Роллета – инженерно-техническое средство защиты, предназначенное для перекрытия и защиты проема в ограждающей конструкции и состоящее из роллетного полотна и устройств для управления перемещением полотна вдоль проема.

Техническая система охраны (система охраны) – совокупность совместно действующих технических средств охраны, установленных на охраняемом объекте и объединенных системой инженерных сетей и коммуникаций

(системы тревожной сигнализации, передачи извещений, контроля и управления доступом, телевизионные системы видеонаблюдения и т. п.).

Технические средства охраны – конструктивно законченные, выполняющие самостоятельные функции устройства, в том числе аппаратно-программные, входящие в состав системы охраны объектов и физических лиц.

Техническая укрепленность – свойство объекта, характеризующее его способность противодействовать его несанкционированному проникновению и противоправным посягательствам, в том числе применению инженерно-технических средств защиты.

Последствия неконтролируемого доступа на объекты различного назначения. Физический доступ человека со злым умыслом на территорию объектов может приводить к различным нежелательным последствиям.

1. Техногенная катастрофа. Последствия от такого воздействия может привести к гибели людей, а в случае аварий на предприятиях химической промышленности – массовой гибели людей, а также существенному загрязнению среды их обитания. Ликвидация подобных последствий требует значительных ресурсов: людских, финансовых и в том числе времени.

2. Хищение материальных ценностей. Последствия такого воздействия – экономические, т. е. финансовый ущерб, а в некоторых случаях и репутационный ущерб, что в конечном итоге приведет к финансовым потерям.

3. Утечка информации. В данном случае, чтобы определить последствия, необходимо понимать, какой категории информация попала третьим лицам. Дальнейшее использование полученных нарушителем сведений может приводить к реализации угроз конфиденциальности, целостности, сохранности и подлинности. Вместе с тем воздействие нарушителя на носитель информации, например удаление данных, приведет к реализации угрозы доступности.

Как было отмечено выше, для оценки последствий необходимо оценивать ущерб от их воздействия, а целенаправленное противодействие угрозам безопасности информации возможно только после их анализа. В случае возможности физического доступа нарушителя на объекты различного назначения система защиты информации проектируется исходя из тех угроз, которые может создать нарушитель. В основе построения системы физической защиты объектов закладываются определенные принципы.

Основные принципы физической защиты объектов. Стратегическая цель при построении системы физической защиты объектов – создание контролируемой зоны на территории объекта. На этой территории размещаются материально-технические ценности, которые имеют определенную ценность для предприятия и проводятся определенные виды работ сотрудниками организации. Поэтому территория объекта делится на зоны. Уровень безопасности каждой зоны, а по сути, комплекс организационно-технических мероприятий, реализуемых в ней, определяется ценностью информации или размещаемых на ее территории ресурсов. Разделение территории объекта на зоны составляет суть принципа **многозональности**. В зависимости от архитектурных особенностей объекта зоны делятся на **следующие виды.**

1. Независимые контролируемые зоны. Создаются для разделения зданий и помещений, в которых сотрудники организации выполняют существенно различающиеся по содержанию и доступу работы (рис. 7.1). Техническая укрепленность одной зоны не зависит от технической укрепленности другой зоны. Примерами таких зон могут быть: здание администрации организации, здание, где располагаются производственные помещения, здание испытательной лаборатории или, если здание одно, помещения, где размещается администрация организации, производственные помещения, помещение испытательной лаборатории.

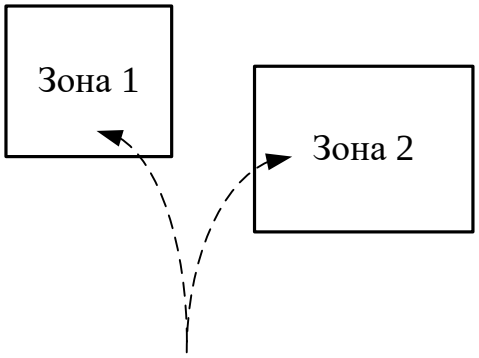


Рис. 7.1. Схематичное изображение движения нарушителя
по направлению к независимым контролируемым зонам

2. Пересекающиеся контролируемы зоны. Формируются в результате наличия смежных помещений, характеризующихся различной технической укрепленностью. В данном случае (рис. 7.2) перемещение нарушителя по территории объекта возможно из зоны 2 в зону 1, исходя из архитектурных особенностей размещения помещений. Примером таких зон может быть смежные помещения: кабинет руководителя организации и приемная.

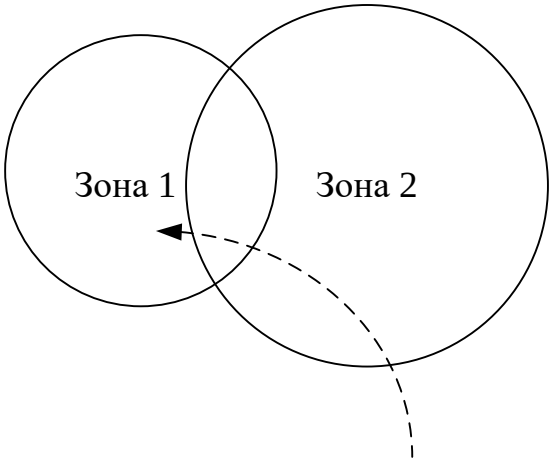


Рис. 7.2. Схематичное изображение движения нарушителя
через пересекающиеся контролируемые зоны

3. Вложенные контролируемые зоны. Формируются в рамках одного объекта и предполагают последовательное перемещение нарушителя из зоны 1 в зону *i* (рис. 7.3). По сути, в данном случае число смежных зон более двух. Примером может служить реализация принципа многозональности в филиале банка. В зону 1 могут входить не только сотрудники банка, но и посетители, однако в этой зоне ведется наблюдение и используются технические средства охраны. Вход из зоны 1 в последующие зоны – контролируемый. Существуют такие зоны, в которые могут войти только те сотрудники, которые там работают.

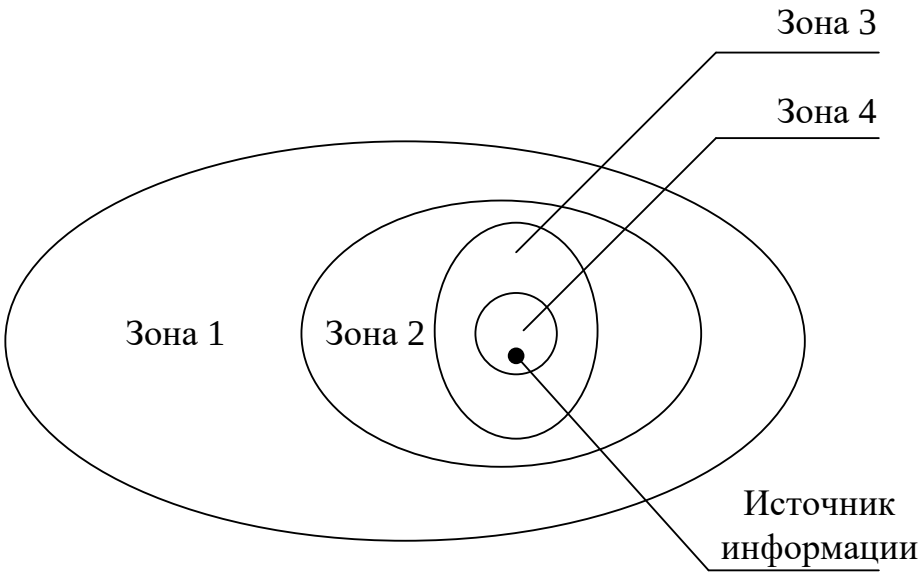


Рис. 7.3. Схематичное изображение движения нарушителя через вложенные контролируемые зоны

Таким образом, контролируемая зона характеризуется:

– методами и средствами контроля доступа;

– используемыми средствами защиты информации;

– реализованными организационными мероприятиями по работе с информацией и ее защите.

Каждая контролируемая зона объекта делится на отдельные рубежи – таким образом реализуется принцип **многорубежности**. При реализации данного принципа контролируется вход нарушителя в зону, его перемещение по ней, его физический доступ к информации, например хранимой на бумаге – в сейфе, т. е. возникает необходимость контролировать предметы. Исходя из чего, существуют следующие рубежи физической защиты:

– периметр (контроль периметра объекта позволяет обеспечить обнаружение нарушителя при его пересечении);

– объем (обеспечивается контроль перемещения нарушителя по площади охраняемого объекта);

– предмет (контроль предметов с целью обнаружения взаимодействия нарушителя с ними). Возьмем, например, банкомат. Он является весьма привлекательным для нарушителей ввиду наличия в его сейфе денежных средств. Исходя из

чего, необходимо контролировать вскрытие сейфа. Но это оказывается недостаточным: группа нарушителей может его взять и унести. Поэтому необходимо контролировать его отрыв от поверхности, на которой он установлен.

Третий принцип – **равнопрочность**. Данный принцип относится к каждому рубежу физической защиты, техническая укрепленность которого по всему протяжению должна быть однородной, а это значит, что рубеж должен быть оборудован средствами защиты, имеющими одинаковые технические характеристики. Нарушитель, планируя проникновение на территорию объекта, будет наблюдать за периметром объекта и собирать информацию о защите остальных рубежей. Такая его деятельность направлена на поиск слабых мест в физической защите рубежей.

Периметр объекта. В случае если объект – это здание или помещение, то периметр объекта представлен их ограждающими конструкциями (стены, потолок и пол). Функционирование организации требует различных ресурсов, например электроэнергии. Электропитание объектов обеспечивается от трансформаторной понижающей подстанции, которая на своем выходе формирует напряжение 380 В переменного тока. Вывод нарушителем подстанции из строя приводит к невозможности энергоснабжения объекта. Поэтому на таких объектах, где отсутствие электроэнергии приводит к тяжким последствиям, трансформаторная подстанция размещается в непосредственной близости от зданий объекта, а по периметру его территории возводится инженерное заграждение. Оно выполняет роль преграды для нарушителя, и его установка позволяет ограничить возможные способы его преодоления нарушителем.

Пути проникновения нарушителя на территорию охраняемого объекта. Создание преград на пути нарушителя будет его вынуждать их преодолевать, если он действует целенаправленно. Обсудим пути его проникновения на территорию объекта.

1. Преодоление ограждения территории объекта.

Существуют следующие способы его преодоления нарушителем:

– преодоление через верх (нарушитель может перелезть через него);

– воздействие на полотно (нарушитель может попытаться проломать ограждение или, если оно сетчатое, вырезать в полотне отверстие, достаточное для того, чтобы он пролез в него);

– подкоп (нарушитель с помощью, например, лопаты может вырыть тоннель под ограждением).

Любое ограждение характеризуется временем сопротивления – временем, которое необходимо потратить нарушителю на его преодоление. Вместе с тем установка ограждения позволяет однозначно оценить способы его преодоления, а соответственно, используя технические средства охраны, обеспечить установление факта преодоления периметра объекта.

2. Проникновение на территорию здания и в помещения здания.

Ограждающие конструкции здания и помещений содержат дверные и оконные проемы, через которые нарушитель может проникнуть. Поэтому, чтобы затруднить, а иногда и исключить (в случае если нарушитель не обладает

необходимыми техническими средствами, которые позволят ему справиться с преградой, и навыками пользования такими средствами) процесс его проникновения, используют инженерно-технические средства защиты оконных и дверных проемов. Например, на оконные проемы устанавливаются роллеты (рис. 7.4), решетки, жалюзи или используется защитное остекление – например, триплекс (рис. 7.5).

Если нарушитель проник на территорию здания, то проникновение его в отдельные помещения возможно через вентиляционные каналы, если эти каналы имеют достаточное для его перемещения сечение.

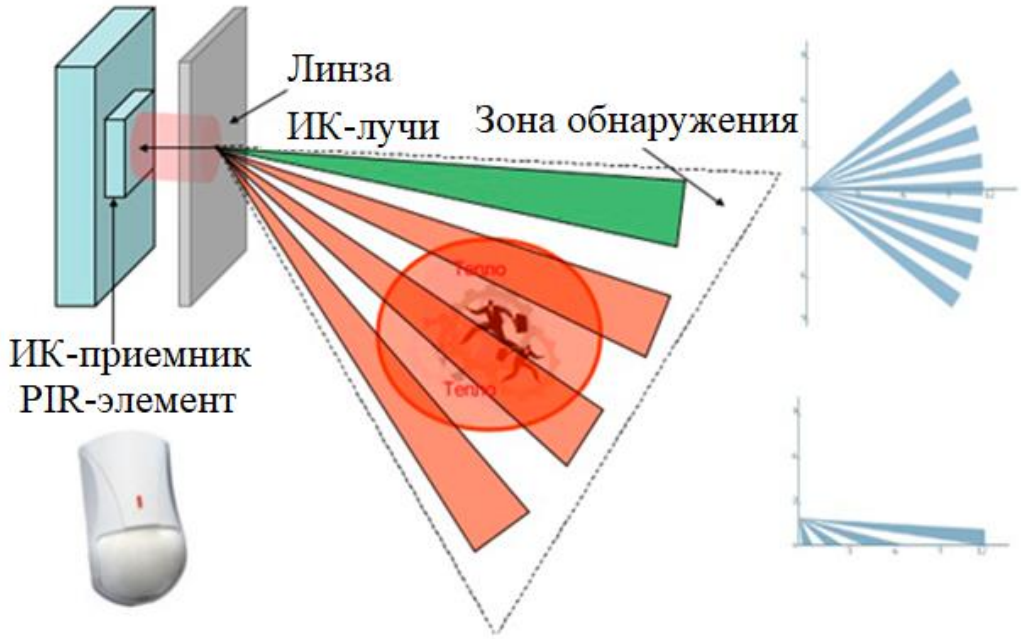
Рис. 7.4. Внешний вид установленной на оконный проем роллеты

а *б*

Рис. 7.5. Схематичное изображение конструкции (*а*)
и внешний вид (*б*) триплекса

Техническую укрепленность дверных проемов обеспечивают за счет использования соответствующего класса защиты дверей. Следует заметить, что если нарушитель действует целенаправленно, имеет необходимые навыки пре-

одоления средств инженерно-технической защиты, то он попадет в контролируемую зону. Поэтому для обнаружения нарушителя применяют технические средства охраны, которые позволяют контролировать пересечение им периметра объекта. Например, для обнаружения перемещения нарушителя внутри помещения используют пассивные инфракрасные средства обнаружения с диаграммой направленности «штора» (рис. 7.6).



PIR – Passive Infrared Motion Sensor
(пассивный инфракрасный датчик движения)

Рис. 7.6. Внешний вид и принцип функционирования пассивного инфракрасного средства обнаружения нарушителя с диаграммой направленности «штора»

Контрольные вопросы

1. Что такое техническая система охраны?
2. Какие можно выделить последствия неконтролируемого доступа на объекты различного назначения?
3. Какие выделяют основные принципы физической защиты объектов?
4. На какие виды делятся контролируемые зоны?
5. Какие существуют пути проникновения нарушителя на территорию охраняемого объекта?

8. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Основная терминология темы. **Криптография** (от др.-греч. κρυπτός – «скрытый» и γράφω – «пишу») – это наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, шифрования.

Конфиденциальность данных – это статус, предоставленный данным и определяющий требуемую степень их защиты.

Целостность данных обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении от данных в исходных документах, т. е. если не произошло их случайного или преднамеренного искажения или разрушения.

Важно отметить, что проблемы конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

Аутентификация (от греч. αὐθεντικός – «реальный, подлинный») – это процедура проверки подлинности, например:

– проверка подлинности пользователя путем сравнения введенного им пароля (для указанного логина) с паролем, сохраненным в базе данных пользовательских логинов;

– подтверждение подлинности электронного документа путем проверки электронной цифровой подписи этого документа по открытому ключу отправителя;

– проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

Шифрование – это обратимое преобразование информации в целях сокрытия от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней.

Цели и задачи криптографической защиты информации. Криптографические методы и средства в основном применяют для обеспечения конфиденциальности информации, контроля целостности данных, а также для решения задач взаимной аутентификации абонентов, т. е. установления, действительно ли пользователь является именно тем, за кого он себя выдает [7–15].

Шифр Цезаря. Шифр Цезаря является частным случаем шифра простой замены. Свое название шифр получил по имени римского императора Гая Юлия Цезаря, который использовал его при переписке с Цицероном (≈50 г. до н. э.) [7].

Сущность шифрования заключается в следующем. Каждую букву исходного текста заменяют на другую букву того же алфавита. Заменяющая буква определяется путем смещения по алфавиту от исходной буквы на K букв. При достижении конца алфавита выполняется циклический переход к его началу. Такой шифр замены можно задать таблицей подстановок, содержащей соответствующие пары букв открытого текста и шифртекста. Совокупность возможных подстановок для $K = 3$ показана в табл. 8.1.

Таблица 8.1

Соответствие между английский алфавитом и множеством целых

Буква		Буква		Буква	
исходная	зашифрованная	исходная	зашифрованная	исходная	зашифрованная
A	*D*	*J*	*M*	*S*	*V*
B	*E*	*K*	*N*	*T*	*W*
C	*F*	*L*	*O*	*U*	*X*
D	*G*	*M*	*P*	*V*	*Y*
E	*H*	*N*	*Q*	*W*	*Z*
F	*I*	*O*	*R*	*X*	*A*
G	*J*	*P*	*S*	*Y*	*B*
H	*K*	*Q*	*T*	*Z*	*C*
I	*L*	*R*	*U*		

Примечание: смещение $K = 3$.

Например, послание Цезаря «VENI VIDI VICI» (в переводе на русский означает «Пришел, увидел, победил»), направленное его другу Аминтию после победы над понтийским царем Фарнаком, выглядело в зашифрованном виде так: «YHQL YLGL YLFL».

Система шифрования Вижинера. Данная система является примером реализации шифра сложной замены [7]. Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены можно описать таблицей шифрования, называемой таблицей (квадратом) Вижинера. Эта таблица используется как для шифрования, так и для расшифрования.

На рис. 8.1 и 8.2 показаны таблицы Вижинера для русского и английского алфавитов соответственно.

В процессе шифрования в верхней строке таблицы находят очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

Рассмотрим пример получения шифртекста с помощью таблицы Вижинера, если необходимо зашифровать сообщение «ПРИЛЕТАЮ СЕДЬМОГО», а в качестве ключевого слова выбрано слово «АМБРОЗИЯ». Чтобы выполнить зашифрование, вначале выпишем исходное сообщение в строку и запишем под ним ключевое слово с повторением. В третью строку будем выписывать буквы шифртекста, определяемые из таблицы Вижинера, как показано на рис. 8.3.

Для получения первой буквы шифртекста в таблице Вижинера (см. рис. 8.1) в верхней строке с подчеркнутыми буквами находят первую букву исходного сообщения (букву П), определяют значение ключа (букве А ключа соответствует число 0, см. табл. 8.2) и находят букву шифртекста, располагающуюся на пересечении буквы П и числа 0 (буква П) и т. д., последняя буква шифртекста (буква Н) находится на пересечении О (буква исходного сообщения) и 31 (число, соответствующее букве Я ключа, см. табл. 8.2).

Ключ	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
0	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
1	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а
2	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б
3	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в
4	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г
5	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д
6	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е
7	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж
8	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з
9	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и
10	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й
11	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
12	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л
13	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м
14	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н
15	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о
16	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
17	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
18	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с
19	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т
20	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
21	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
22	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
23	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
24	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
25	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
26	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
27	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
28	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы
29	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ
30	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э
31	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю

Рис. 8.1. Таблица Вижинера для русского алфавита

Ключ	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
2	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
3	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
4	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
5	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
6	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
7	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
8	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
10	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
11	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
12	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
13	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
14	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
16	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
17	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
18	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
19	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
20	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
21	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
22	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
23	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
24	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
25	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Рис. 8.2. Таблица Вижинера для английского алфавита

Сообщение	П	Р	И	Л	Е	Т	А	Ю		С	Е	Д	Ь	М	О	Г	О
Ключ	А	М	Б	Р	О	З	И	Я		А	М	Б	Р	О	З	И	Я
Шифртекст	П	Ъ	Й	Ы	У	Щ	И	Э		С	С	Е	К	Ь	Х	Л	Н

Рис. 8.3. Система шифрования Вижинера

Таблица 8.2

Соответствие между русским алфавитом и множеством целых

Буква	Число	Буква	Число	Буква	Число	Буква	Число
А	0	И	8	Р	16	Ш	24
Б	1	Й	9	С	17	Щ	25
В	2	К	10	Т	18	Ь	26
Г	3	Л	11	У	19	Ы	27
Д	4	М	12	Ф	20	Ъ	28
Е	5	Н	13	Х	21	Э	29
Ж	6	О	14	Ц	22	Ю	30
З	7	П	15	Ч	23	Я	31

Криптоатака и криптоанализ. **Криптоаналитическая атака** – это любая попытка со стороны перехватчика расшифровать шифртекст для получения открытого текста или зашифровать свой собственный текст для получения правдоподобного шифртекста, не имея подлинного ключа.

Криптоанализ – это наука о методах расшифрования зашифрованной информации без доступа к криптографическому ключу, а также сам процесс такого расшифрования.

Основные методы криптоанализа включают криптоаналитическую атаку [7–15]:

– на основе шифртекста;

– на основе открытых текстов и соответствующих шифртекстов;

– при возможности выбора открытого текста;

– с адаптивным выбором открытого текста;

– с использованием выбранного шифртекста;

– методом полного перебора всех возможных ключей.

Симметричная криптосистема. Обобщенная схема симметричной криптографической системы, обеспечивающей шифрование передаваемой информации, показана на рис. 8.4.

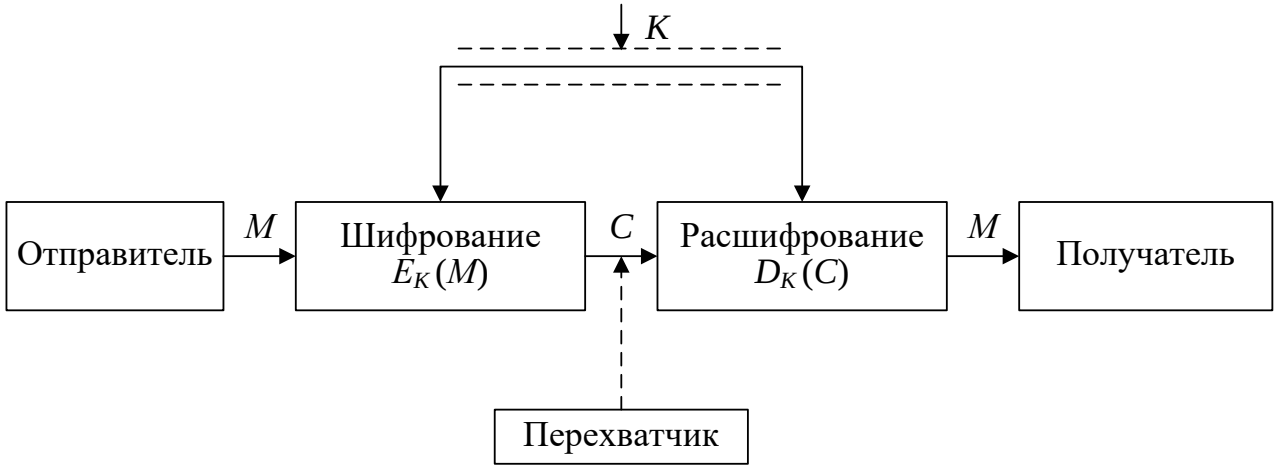


Рис. 8.4. Обобщенная схема криптографической системы

Отправитель генерирует открытый текст исходного сообщения M, которое должно быть передано законному получателю по незащищенному каналу связи. За каналом связи следит перехватчик с целью перехватить и раскрыть передаваемое сообщение. Для того чтобы перехватчик не смог узнать содержание сообщения M, отправитель шифрует его с помощью обратимого преобразования E_K и получает шифртекст (или криптограмму) $C = E_K(M)$, который (которую) отправляет получателю.

Законный получатель, приняв шифртекст C, расшифровывает его с помощью обратного преобразования $D = E_K^{-1}$ и получает исходное сообщение в виде открытого текста M:

$$D_K\left(C\right) = E_K^{-1}\left(E_K\left(M\right)\right) = M. \qquad (8.1)$$

Преобразование E_K выбирается из семейства криптографических преобразований, называемых **криптоалгоритмами**. Параметр, с помощью которого выбирается отдельное используемое преобразование, называется **криптографическим ключом *K*.**

Важно отметить, что криптосистема может иметь различные варианты реализации (набор инструкций, аппаратные средства, комплекс программ компьютера, программно-аппаратный комплекс), которые позволяют зашифровать открытый текст и расшифровать шифртекст различными способами, один из которых выбирается с помощью конкретного ключа *K*.

Асимметричная криптосистема. Обобщенная схема асимметричной криптосистемы с двумя разными ключами K_1 и K_2 показана на рис. 8.5.

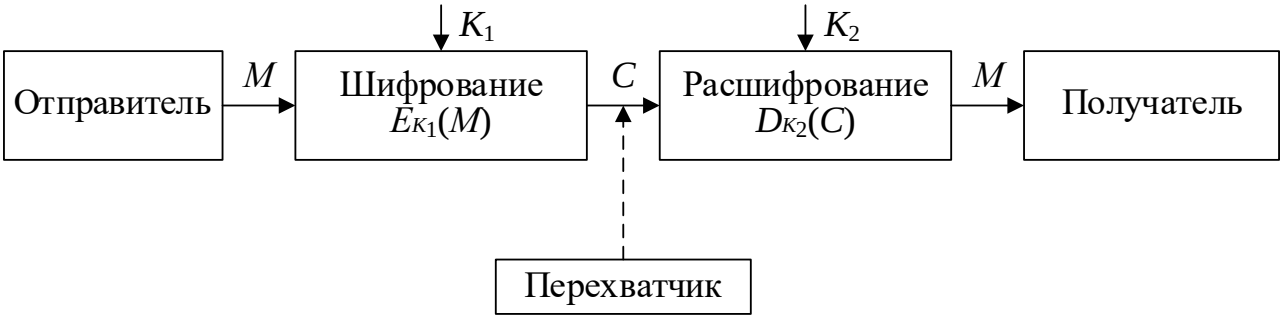


Рис. 8.5. Обобщенная схема асимметричной криптосистемы с открытым ключом

В асимметричной криптосистеме один из ключей является открытым, а другой – личным. Причем по незащищенному каналу передается только открытый ключ, а личный ключ сохраняют на месте его генерации [7–15].

Протокол Диффи – Хеллмана. Данный протокол (рис. 8.6) применяют в системах открытого распределения ключей. Информационная безопасность протокола Диффи – Хеллмана обусловлена трудностью вычисления дискретных логарифмов в конечном поле.

Предположим, что два пользователя *A* и *B* хотят организовать защищенный коммуникационный канал. В этом случае протокол Диффи – Хеллмана включает следующие этапы (см. рис. 8.6).

Этап 1. Обе стороны заранее уславливаются о модуле N (N должен быть простым числом) и примитивном элементе $g \in Z_N$, $1 \le g \le (N-1)$, степени которого образуют все ненулевые элементы множества Z_N, т. е.

$$\left\{g^1, g^2, ..., g^{N-1} = 1\right\} = Z_N - \{0\}. \qquad (8.2)$$

Два целых числа N и g могут не храниться в секрете. Как правило, указанные значения являются общими для всех пользователей системы.

Этап 2. Пользователи A и B независимо друг от друга выбирают собственные личные ключи k_A и k_B (k_A и k_B – случайные большие целые числа, которые хранятся пользователями A и B в секрете).

Этап 3. Пользователь A вычисляет открытый ключ

$$y_A = g^{k_A} \pmod N, \tag{8.3}$$

и пользователь B вычисляет открытый ключ

$$y_B = g^{k_B} \pmod N. \tag{8.4}$$

Этап 4. Пользователи A и B обмениваются вычисленными значениями открытых ключей y_A и y_B по незащищенному каналу (будем считать, что все данные, передаваемые по незащищенному каналу связи, могут быть перехвачены злоумышленником).

Этап 4. Пользователи A и B вычисляют общий личный ключ, используя следующие сравнения:

$$\text{пользователь } A\text{: } K \equiv \left(y_B\right)^{k_A} \equiv \left(g^{k_B}\right)^{k_A} \pmod N, \tag{8.5}$$

$$\text{пользователь } B\text{: } K' \equiv \left(y_A\right)^{k_B} \equiv \left(g^{k_A}\right)^{k_B} \pmod N. \tag{8.6}$$

При этом $K = K'$, так как $\left(g^{k_B}\right)^{k_A} \pmod N = \left(g^{k_A}\right)^{k_B} \pmod N$.

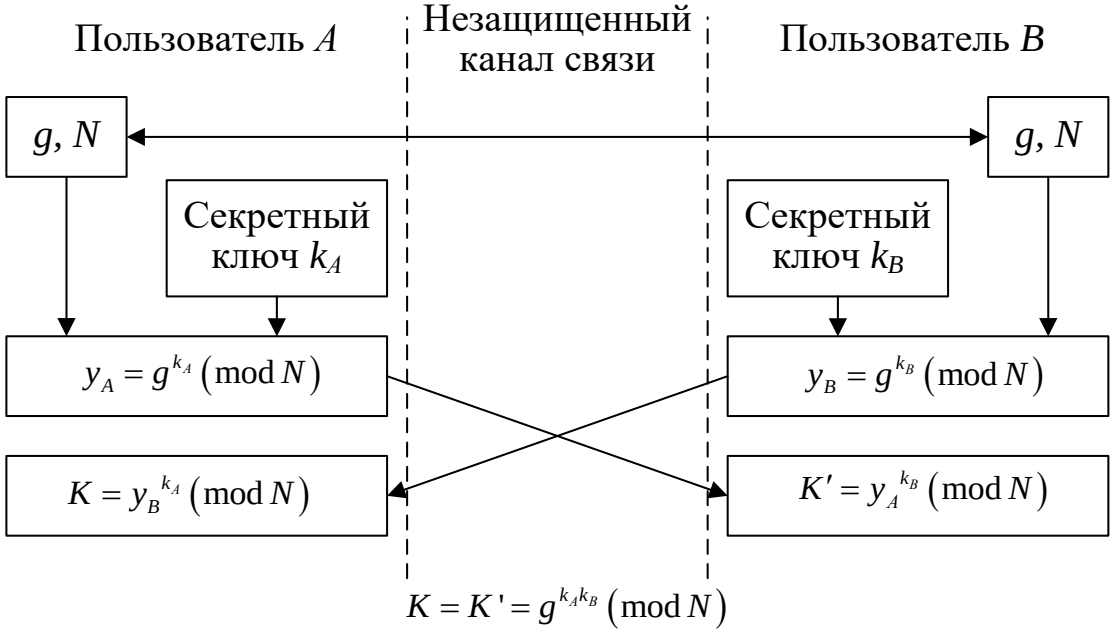


Рис. 8.6. Схема реализации протокола Диффи – Хеллмана

Отметим, что ключ *K* может использоваться в качестве общего личного ключа (ключа шифрования ключей) в симметричной криптосистеме.

Атака «человек посередине» (MITM). **Атака «человек посередине» (англ. Man in the Middle, MITM), или атака посредника** – это вид атаки, при которой злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом.

Такая атака является методом компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию.

Одним из примеров атак типа «человек посередине» является активное прослушивание, при котором злоумышленник устанавливает независимые связи с жертвами и передает сообщения между ними. Тем самым он заставляет жертв поверить, что они разговаривают непосредственно друг с другом через частную связь, а фактически весь разговор управляется злоумышленником [11].

Атака обычно начинается с прослушивания канала связи и заканчивается тем, что криптоаналитик пытается подменить перехваченное сообщение, извлечь из него полезную информацию, перенаправить его на какой-нибудь внешний ресурс.

Рассмотрим следующий пример. Предположим, пользователь *A* планирует передать пользователю *B* некоторую информацию. Пользователь *C* обладает знаниями о структуре и свойствах используемого метода передачи данных, а также о факте планируемой передачи информации. Для совершения атаки пользователь *C* «представляется» пользователю *A* как пользователь *B*, а пользователю *B* – как *A*. Пользователь *A*, ошибочно полагая, что он направляет информацию пользователю *B*, посылает ее пользователю *C*. Пользователь *C*, получив информацию и совершив с ней некоторые действия (например, скопировав или модифицировав информацию в своих целях), пересылает информацию получателю – в рассматриваемом примере пользователю *B*. Пользователь *B*, в свою очередь, считает, что информация была получена им напрямую от пользователя *A*.

Сертификат открытого ключа. Подмена сертификата открытого ключа. Сертификат открытого ключа (сертификат электронной цифровой подписи, или сертификат ключа подписи, или сертификат ключа проверки электронной подписи) – это электронный или бумажный документ, содержащий открытый ключ, информацию о владельце ключа, области применения ключа, подписанный выдавшим его Удостоверяющим центром и подтверждающий принадлежность открытого ключа владельцу.

Открытый ключ может быть использован для организации защищенного канала связи с владельцем двумя способами [7–15]:

– для проверки подписи владельца (решается задача аутентификации отправителя данных);

– для шифрования посылаемых ему данных (решается задача обеспечения конфиденциальности передаваемой информации).

Сертификат представляет собой электронную форму, в которой содержится следующая информация:

– открытый ключ владельца данного сертификата;

– сведения о владельце сертификата (например, имя, адрес электронной почты, наименование организации, в которой он работает и т. п.);

– наименование сертифицирующей организации, выдавшей данный сертификат;

– электронная подпись сертифицирующей организации, т. е. зашифрованные личным ключом этой организации данные, содержащиеся в сертификате.

Чтобы исключить подмену сертификата открытого ключа важно, чтобы Удостоверяющий центр (сертифицирующая организация) выполнил (выполнила) первичную аутентификацию стороны, которой выдается этот сертификат.

Функции сертифицирующей организации могут выполнять:

– предприятие, которое обеспечивает сертификатами своих сотрудников;

– независимые центры по выдаче сертификатов, работающие на коммерческой основе.

В соответствии со стандартом X.509 сектора телекоммуникационной стандартизации международного союза электросвязи ITU-T (International Telecommunications Union – Telecommunication Standardization Sector) цифровые сертификаты могут быть следующих классов:

Сертификаты класса 1 предоставляют пользователю самый низкий уровень полномочий. Они могут применяться при отправке и получении шифрованной электронной почты через Интернет.

Чтобы получить сертификат этого класса, пользователь должен сообщить сертифицирующей организации свой адрес электронной почты или свое уникальное имя.

Сертификаты класса 2 позволяют владельцам пользоваться внутрикорпоративной электронной почтой и принимать участие в подписных интерактивных службах.

Чтобы получить сертификат этого более высокого уровня, пользователь должен организовать подтверждение своей личности сторонним лицом, например своим работодателем. Такой сертификат с информацией от работодателя может эффективно применяться при деловой переписке.

Сертификаты класса 3 предоставляют владельцу все те возможности, которые имеет обладатель сертификата класса 2, а также возможность участия в электронных банковских операциях, электронных сделках по покупке товаров и некоторые другие возможности [12].

Для доказательства своей аутентичности соискатель сертификата должен явиться лично и предоставить подтверждающие документы.

Сертификаты класса 4 используются при выполнении крупных финансовых операций. Поскольку такой сертификат наделяет владельца самым высо-

ким уровнем доверия, сертифицирующая организация проводит тщательное изучение частного лица или организации, запрашивающей сертификат.

Сертификаты можно использовать не только для аутентификации, но и для предоставления избирательных прав доступа. Для этого в сертификат могут вводиться дополнительные поля, в которых указывается принадлежность его владельцев к той или иной категории пользователей. Эта категория назначается сертифицирующей организацией в зависимости от условий, на которых выдается сертификат. Например, организация, поставляющая через Интернет на коммерческой основе информацию, может выдавать сертификаты определенной категории пользователям, оплатившим годовую подписку на некоторый бюллетень, тогда веб-сервер будет предоставлять доступ к страницам бюллетеня только пользователям, предъявившим сертификат данной категории [7–15].

Электронная цифровая подпись (ЭЦП). Согласно терминологии, утвержденной Международной организацией по стандартизации ISO (International Organization for Standardization / International Standards Organization), под термином «**цифровая подпись**» понимаются методы, позволяющие устанавливать подлинность автора сообщения (документа) при возникновении спора относительно авторства.

Система ЭЦП включает две процедуры:

– процедуру постановки подписи;

– процедуру проверки подписи.

Обобщенная схема формирования и проверки цифровой подписи показана на рис. 8.7.

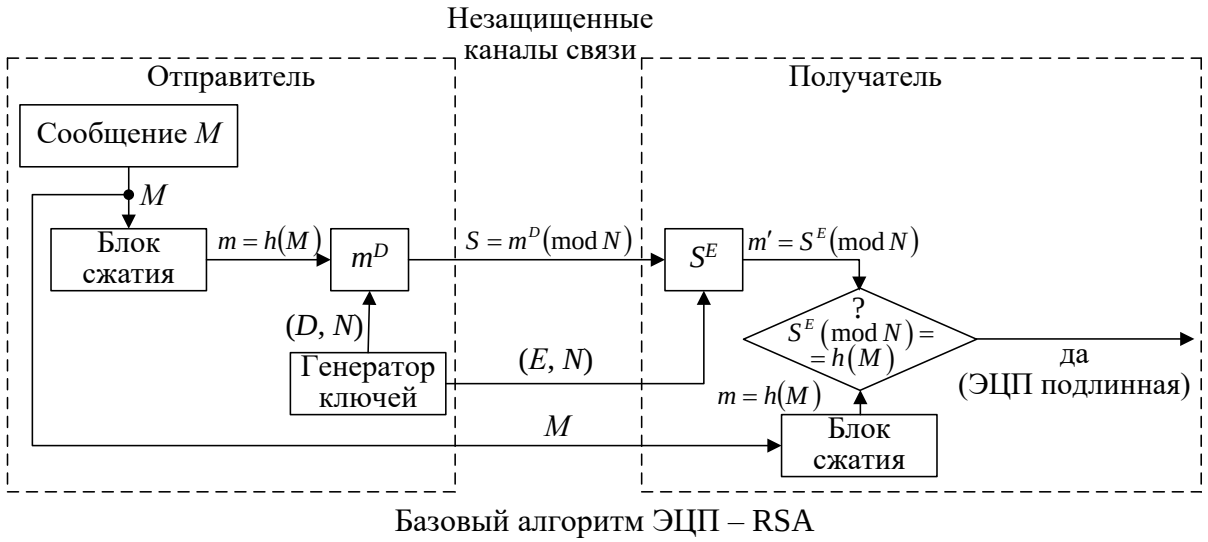


Рис. 8.7. Обобщенная схема цифровой подписи [7–15]

Рассмотрим принципы функционирования схемы, приведенной на рис. 8.7. Допустим, что отправитель хочет подписать сообщение M перед его отправкой. Сначала сообщение M (блок информации, файл, таблица и т. п.) сжимают с помощью хеш-функции h в целое число m:

$$m = h(M). \tag{8.7}$$

Затем вычисляют цифровую подпись S под электронным документом M, используя хеш-значение m и личный ключ D:

$$S = m^D \left(\mathrm{mod}\, N\right), \tag{8.8}$$

где N – модуль, который определяют как произведение различных случайных больших простых чисел P и Q.

Личный ключ D вычисляют с использованием расширенного алгоритма Евклида как мультипликативную инверсию открытого ключа E по модулю функции Эйлера:

$$\varphi(N) = (P-1)\cdot(Q-1). \tag{8.9}$$

Пара (M, S) передается партнеру-получателю как электронный документ M, подписанный цифровой подписью S. Причем подпись S сформирована обладателем личного ключа D.

После приема пары (M, S) получатель вычисляет хеш-значение сообщения M двумя разными способами. Прежде всего он восстанавливает хеш-значение m' применяя криптографическое преобразование подписи S с использованием открытого ключа E:

$$m' = S^E (\mathrm{mod}\, N). \tag{8.10}$$

Кроме того, он находит результат хеширования принятого сообщения M с помощью такой же хеш-функции $m = h(M)$. Если соблюдается равенство вычисленных значений, то получатель признает пару (M, S) подлинной. Для рассматриваемого примера (см. рис. 8.7) доказано, что только обладатель личного ключа D может сформировать цифровую подпись S по документу M. Также доказано, что определить секретное число D по открытому числу E не легче, чем разложить модуль N на множители.

Стеганогра́фия (от греч. στεγανός – «скрытый» и γράφω – «пишу») – это способ передачи или хранения информации с учетом сохранения в тайне самого факта такой передачи (хранения).

В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например как изображение, статья или некий список [8]. Стеганографию можно использовать совместно с методами криптографии, таким образом дополняя ее.

Преимущество стеганографии над «чистой» криптографией состоит в том, что сообщения не привлекают к себе внимания. Таким образом, крипто-

графия защищает содержание сообщения, а стеганография – сам факт наличия каких-либо скрытых посланий [8].

Важно отметить, что в Республике Беларусь определены следующие основные технические нормативные правовые акты в области криптографической защиты информации:

1. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

2. РД РБ 07040.1202-2003 «Банковские технологии. Процедура выработки псевдослучайных данных с использованием секретного параметра».

3. СТБ 34.101.27-2012 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации».

4. СТБ П 34.101.43-2009 «Информационные технологии. Методы и средства безопасности. Профиль защиты технических и аппаратно-программных средств криптографической защиты информации» (задание по безопасности).

5. СТБ 34.101.18-2009 «Информационные технологии. Синтаксис обмена персональной информацией» с учетом использования ГОСТ 28147, СТБ 34.101.31-2011.

6. СТБ П 34.101.23-2008 «Информационные технологии. Защита информации. Форматы параметров криптографических алгоритмов» с учетом использования ГОСТ 28147, СТБ 34.101.31-2011.

7. СТБ 1176.1-99 «Информационная технология. Защита информации. Процедура хэширования».

8. СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи».

9. СТБ П 34.101.45-2011 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи на основе эллиптических кривых».

10. РД РБ 07040.1204-2004 «Банковские технологии. Формат карточки открытого ключа».

11. СТБ 34.101.17-2009 «Информационные технологии. Синтаксис запроса на получение сертификата» с учетом использования СТБ 1176.1-99, СТБ 1176.2-99, СТБ 34.101.31-2011.

12. СТБ 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности».

Контрольные вопросы

1. Что называется перехватом информации?

2. Какое условие необходимо выполнить для организации процесса перехвата информации?

3. Какое наименование носит прямое и обратное криптографическое преобразование информации?

4. В чем заключаются основные особенности симметричных криптосистем?

5. В чем заключаются основные преимущества использования асимметричных криптосистем по сравнению с симметричными криптосистемами?

6. В каких случаях целесообразно применять симметричные криптосистемы, а в каких – асимметричные?

7. Для чего используют протокол Диффи – Хеллмана?

8. В чем заключается сущность атаки «человек посередине» (MITM)?

9. Какие классы цифровых сертификатов определены стандартом X.509 ITU-T?

10. Каким образом противодействуют анализу потока сообщений?

9. ЗАЩИТА ИНФОРМАЦИИ ОТ ТЕХНИЧЕСКОЙ РАЗВЕДКИ

Основная терминология темы. **Объект информатизации** – средства электронной вычислительной техники вместе с программным обеспечением, в том числе системы управления различного уровня и назначения, информационные системы и сети, автономные стационарные и персональные электронные вычислительные машины, используемые в соответствии с заданной информационной технологией, системы управления информационными, производственными и (или) технологическими процессами.

Специальная проверка помещения (объекта информатизации) – совокупность мероприятий, реализуемых для обнаружения в помещении (на объекте информатизации) возможных специальных технических средств, предназначенных для негласного получения информации.

Специальное исследование помещения (объекта информатизации) – совокупность мероприятий, реализуемых для выявления технических каналов утечки защищаемой информации в помещении и оценки соответствия мероприятий по защите информации требованиям нормативных правовых актов в сфере защиты информации.

Технический канал утечки информации. По своей сути технические каналы утечки информации являются каналами связи. Как известно, любой канал связи представляет собой совокупность трех элементов:

– источник информации;

– приемник информации;

– среда, по которой информация распространяется или передается от ее источника к ее приемнику (воздух, проводные линии);

Таким образом, представляется вполне логичным определить технический канал утечки информации как совокупность следующих трех элементов:

– источник информации, распространение и (или) предоставление которой ограничено;

– приемник информации, распространение и (или) предоставление которой ограничено (в соответствии с законодательством Республики Беларусь такое устройство следует называть специальным техническим средством, предназначенным для негласного получения информации (далее по тексту – специальное техническое средство));

– среда, по которой информация распространяется (в том числе и в направлении потенциального места установки специального технического средства).

Отметим два отличия технического канала утечки информации от канала связи. Итак, в первом в отличие от второго:

– процесс распространения информации не контролируется ее обладателем;

– среда, по которой информация распространяется, выходит за границы контролируемой зоны периметра, в пределах которого располагается источник информации.

Таким образом, под утечкой информации следует понимать:

– явление неконтролируемого распространения информации, распространение и (или) предоставление которой ограничено;

– явление неконтролируемого распространения за границы контролируемой зоны информационных сигналов, формируемых источником информации, распространение и (или) предоставление которой ограничено.

К слову о сигналах, формируемых источником информации, распространение и (или) предоставление которой ограничено. В зависимости от их природы принято классифицировать технические каналы утечки информации, подразделяя их:

– на визуально-оптические;

– каналы побочного электромагнитного излучения и наводок;

– акустические.

Нетрудно догадаться, что в визуально-оптическом канале источник информации, распространение и (или) предоставление которой ограничено, формирует информационные сигналы в виде электромагнитных волн оптического диапазона (видимой или инфракрасной областей спектра), в канале побочного электромагнитного излучения и наводок – в виде электромагнитных волн диапазона частот 10 кГц – 2 ГГц, а в акустическом – в виде акустических волн, которые по своей сути являются механическими колебаниями или совокупностью перемещающихся (колеблющихся) частиц среды, по которой эти волны распространяются.

Средой, по которой указанные сигналы распространяются, может быть: газ (как правило, воздух), твердый материал, жидкость, проводные линии.

В табл. 9.1–9.3 представлены характеристики каждого из технических каналов утечки информации.

Акустические каналы утечки информации чаще, чем другие, используются для перехвата информации, распространение и (или) предоставление которой ограничено. Это связано с тем, что более 80 % процессов, связанных с информационным обменом, основано на использовании речевых сообщений, а не бумажных или электронных документов. В связи с этим существует пять подходов к перехвату информации по акустическим каналам ее утечки, каждый из которых соотвествует определенному их виду. Разделение акустических каналов утечки информации на виды реализуется в зависимости от того, что является средой распространения информации и какие специальные технические средства применяются для ее перехвата. В табл. 9.4 представлены характеристики акустических каналов утечки информации каждого из видов.

Таблица 9.1

Характеристики визуально-оптического канала утечки информации

Характеристика источника информации	Объект, характеристики которого представляют собой информацию, распространение и (или) предоставление которой ограничено	
Среда, по которой информация распространяется	Воздух. Твердый материал (прозрачный в оптическом диапазоне длин электромагнитных волн)	
Специальные технические средства	Средства для негласного визуального наблюдения (фотокамеры или видеокамеры, закамуфлированные под предметы другого функционального назначения и (или) имеющие объективы с вынесенным зрачком входа)	
	Тепловизоры	

Таблица 9.2

Характеристики канала побочного электромагнитного излучения и наводок

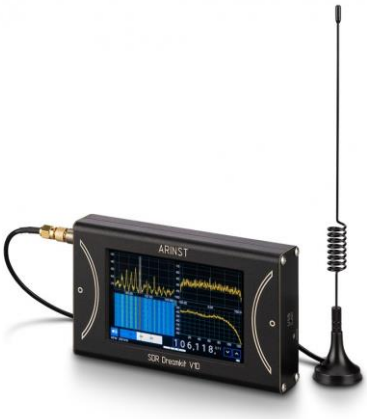
Характеристика источника информации	Средство вычислительной техники, с помощью которого выполняется обработка информации, распространение и (или) предоставление которой ограничено	
Среда распространения	Воздух. Твердый материал (заграждающие конструкции зданий и помещений). Проводные линии	
Специальные технические средства	Антенны, анализаторы спектра, демодуляторы сигналов	

Таблица 9.3

Характеристики акустического канала утечки информации

Наименование канала утечки информации	Акустический
Характеристика источника информации	Человек, располагающий знаниями о содержании информации, распространение и (или) предоставление которой ограничено
Среда распространения	Воздух. Твердый материал (заграждающие конструкции зданий и помещений). Инженерные коммуникации (трубы водоснабжения, отопления, вентиляции). Проводные линии
Специальные технические средства	См. табл. 9.4

Таблица 9.4

Характеристики акустических каналов утечки информации

Наименование акустического канала утечки информации	Среда, по которой информация распространяется	Специальное техническое средство
Прямой акустический	Воздух. Ограждающие конструкции зданий и помещений (стены, потолки, полы, окна)	Акустические закладки (микрофоны, соединенные с миниатюрными звукозаписывающими устройствами и передатчиками и т. п.) 
Виброакустический	Ограждающие конструкции зданий и помещений (стены, потолки, полы, окна). Инженерные коммуникации (трубы водоснабжения, отопления, вентиляции)	Устройства, преобразующие механические колебания твердых материалов в электрические сигналы (электронные стетоскопы, виброметры, акселерометры и т. п.) 

Окончание табл. 9.4

Наименование акустического канала утечки информации	Среда, по которой информация распространяется	Специальное техническое средство
Оптоэлектронный	Оконные стекла	Лазерные микрофоны 
Акустоэлектрический	Электрические цепи, в которых реализуются преобразования электрических сигналов в акустические (явление «микрофонного эффекта»)	Высокочувствительные низкочастотные усилители, генераторы высокочастотного (более 100 кГц) сигнала, приемники-демодуляторы
Параметрический	Электрические цепи, в которых реализуются преобразования электрических сигналов в акустические	Приемники-демодуляторы

Характеристика источников информации. Источниками информации в технических каналах ее утечки являются следующие.

1. Человек. Обнаружение и идентификация человека реализуются по его видовым демаскирующим признакам, к которым относятся его внешний вид и черты лица. Кроме этого, человек является источником речевой информации, как было отмечено выше – наиболее значимого вида сведений.

2. Средства вычислительной техники. Используются человеком для приема, обработки, хранения и передачи информации. К таким средствам относятся персональные компьютеры, принтеры и т. п. В электрических цепях таких устройств протекает переменный ток (электрический сигнал), несущий в себе информацию. Проводник, по которому протекает такой ток, является антенной, и он излучает электромагнитную волну в окружающее его пространство. Вследствие этого формируется электромагнитное поле, регистрация которого позволяет получить информацию, которая передается с помощью электромаг-

нитного излучения средства вычислительной техники. Формируемое электромагнитное излучение принято называть побочным. В помещении, где формируется побочное электромагнитное излучение (ПЭМИ), часто располагаются различные проводные линии, например линия электропитания средств вычислительной техники. Взаимодействие ПЭМИ с такой линией, будет вызывать появление в ней токов высокой частоты за счет наводки ПЭМИ на такую линию. Поэтому перехват информации со средств вычислительной техники в данном случае возможен за счет регистрации наводок ПЭМИ в проводных линиях.

3. Здания и сооружения (внешний вид). Обнаружение таких объектов реализуется по их видовым демаскирующим признакам, иногда по этим признакам можно определить является ли здание административным, производственным или жилым.

Перехват информации при разведывательном контакте с источником информации. Рассмотрим особенности перехвата информации от различных источников с учетом среды ее распространения и используемого для этого специального технического средства.

Источник информации – человек. Для обнаружения и идентификации человека необходимо зафиксировать его видовые демаскирующие признаки, регистрацию которых выполняют с помощью следующих специальных технических средств:

– визуально-оптических (бинокли, стереотрубы и т. п.). Такие технические средства функционируют в диапазоне длин волн 400–750 нм;

– оптоэлектронных (приборы ночного видения, тепловизоры). Приборы ночного видения функционируют в диапазоне длин волн 750–1200 нм и позволяют получать изображения при условиях недостаточной освещенности (при свете Луны и звезд). Тепловизоры имеют диапазоны рабочих длин волн 3–5 мкм и 8–12 мкм и позволяют фиксировать собственное инфракрасное излучение тела человека.

Указанные специальные технические средства регистрируют информацию при ее распространении в воздушной среде.

Перехват речевой информации, формируемой речевым аппаратом человека, ведется в диапазоне частот 125–8000 Гц в воздушной среде с помощью следующих акустических специальных технических средств:

– направленный микрофон (в отличие от обычного микрофона, конструкция направленного позволяет значительной увеличить дальность перехвата информации (рис. 9.1));

– акустических закладок, размещаемых в помещениях, где непосредственно находится человек;

– средств радиоперехвата (рис. 9.2), которые позволяют обеспечить регистрацию электромагнитной волны в диапазоне частот 20 МГц – 12 ГГц, которая распространяется от сотового аппарата человека, который он использует для речевой коммуникации.

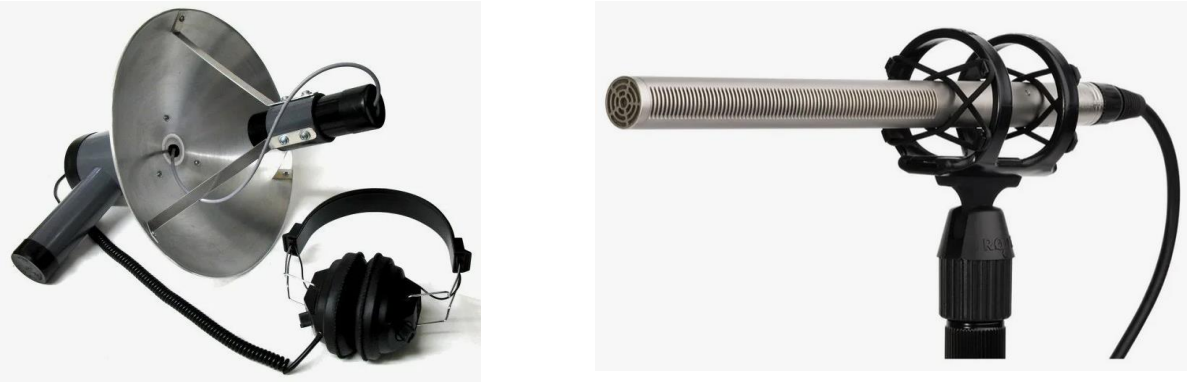


Рис. 9.1. Внешний вид конструкций направленных микрофонов

Рис. 9.2. Внешний вид средства радиоперехвата

При условии, что человек ведет разговор внутри помещения, речевой сигнал в виде акустической волны взаимодействует с ограждающими конструкциями этого помещения и вызывает их вынужденные колебания в диапазоне частот речевого сигнала. Таким образом, средой распространения речевой информации становится твердая среда. Перехват речевой информации в таком случае реализуется со стен, пола и потолков с помощью электронного стетоскопа (рис. 9.3).

Стекла в оконных проемах, как и ограждающие конструкции помещений, также будут под действием акустической волны совершать вынужденные колебания. Для их регистрации используют активную систему – лазерный микрофон (рис. 9.4). Такое специальное техническое средство обеспечивает перехват речевой информации за счет облучения стекла лазером, луч которого будет модулироваться речевым сигналом, и отраженный от стекла луч принимается специальным техническим средством, которое обеспечивает выделение из него речевой информации.

Рис. 9.3. Внешний вид электронного стетоскопа

Рис. 9.4. Внешний вид лазерного микрофона

Для передачи речевых сообщений человек использует средства проводной телефонной связи, поэтому нарушитель может подключиться к линии связи и перехватить речевой сигнал в полосе частот канала связи за счет использования электронных специальных технических средств. В данном случае средой распространения информации является канал связи (электрические цепи).

Источник информации – средства вычислительной техники. Для перехвата информации необходимо обеспечить регистрацию побочных электромагнитных излучений и наводок. Для их регистрации в воздушном пространстве используют средства радиоперехвата, а в проводных линиях (электрических цепях) – электронные специальные технические средства.

Источник информации – здания и сооружения (внешний вид). Для обнаружения зданий и сооружений (выявления их видовых демаскирующих признаков) используют визуально-оптические и оптоэлектронные специальные технические средства, аналогичные тем, которые применяют для обнаружения и идентификации человека. Среда распространения информации – воздушная.

Мероприятия по противодействию технической разведке. Комплекс мероприятий включает в первую очередь активные и пассивные технические методы защиты информации, которые были обсуждены выше, направленные на снижение отношения сигнал/шум на входе приемного устройства специального технического средства.

Необходимо заметить, что специальное техническое средство может быть внесено в контролируемую зону человеком, который имеет туда легальный доступ, и скрытно им установлено для перехвата информации. Для выявления таких специальных технических средств в ограждающих конструкциях, предметах мебели и интерьера помещений проводят **специальные исследования** помещений с помощью технических средств.

Специальное техническое средство для перехвата информации может быть встроено нарушителем в технические средства приема, передачи и обработки информации, и для их обнаружения выполняют **специальные проверки** технических средств приема, передачи и обработки информации.

Специальные исследования проводятся с использованием технических средств и направлены на выявление технических каналов утечки информации и оценку соответствия применяемых мероприятий по защите информации требованиям соответствующих нормативных правовых актов.

Методы защиты информации от утечки по техническим каналам. Методы защиты информации от утечки по техническим каналам должны носить комплексный характер, иными словами, представлять собой совокупность организационных, правовых и технических методов.

Организационные методы защиты информации от утечки по техническим каналам включают в себя такие мероприятия, как:

– выбор размера и формы контролируемой зоны периметра, в пределах которого располагается источник информации, распространение и (или) предоставление которой ограничено, таким образом, чтобы на границе этой зоны формируемые этим источником информационные сигналы характеризовались такой амплитудой, при которой на их основе не представляется возможным восстановление информации;

– выбор места расположения источника информации, распространение и (или) предоставление которой ограничено, в пределах контролируемой зоны таким образом, чтобы значение амплитуды формируемых этим источником информационных сигналов на границах этой зоны была минимальной.

Также можно дополнительно выделить организационные методы защиты информации от утечки по каждому из технических каналов.

В частности, организационные методы защиты информации от утечки по визуально-оптическому каналу включают в себя такие мероприятия, как:

– расположение объекта, характеристики которого представляют собой информацию, распространение и (или) предоставление которой ограничено, на такой местности, которая характеризуются ограниченной обзорностью;

– расположение объекта, характеристики которого представляют собой информацию, распространение и (или) предоставление которой ограничено, в месте, установка специальных технических средств в котором представляется затруднительной.

Организационные методы защиты информации от утечки по каналу побочного электромагнитного излучения и наводок включают в себя такие мероприятия, как:

– выбор для обработки информации, распространение и (или) предоставление которой ограничено, средства вычислительной техники с низким уровнем формируемого его проводными линиями побочного электромагнитного излучения;

– установка средства вычислительной техники, используемого для обработки информации, распространение и (или) предоставление которой ограничено, в точке, которая максимально удалена от проводных линий, выходящих за пределы помещения, в котором расположено указанное средство.

Организационные методы защиты информации от утечки по акустическим каналам включают в себя такие мероприятия, как:

– организация обсуждения информации, распространение и (или) предоставление которой ограничено, в помещениях:

- располагающихся НЕ на первом и НЕ на последнем этаже здания;
- имеющих минимальное количество смежных помещений;
- окна которых выходят во внутренний двор (при наличии такового);

– плотное закрытие окон и дверей помещений, в которых обсуждается информация, распространение и (или) предоставление которой ограничено;

– установка стола для проведения переговоров в точке, которая максимально удалена от окон и дверей помещения, а также телефонных аппаратов и проводных линий, расположенных в пределах этого помещения;

– снижение громкости речи участниками обсуждения информации, распространение и (или) предоставление которой ограничено.

Технические методы защиты информации от утечки по техническим каналам основаны на использовании технических средств защиты информации, представленных в разделе 5 «Методы защиты информации». В указанном разделе также приведены нормативные правовые акты, содержание которых является основой для реализации правовых методов защиты информации от утечки по техническим каналам.

Также можно выделить организационно-технические методы защиты информации от утечки по техническим каналам. К ним относятся специальная проверка помещения (объекта информатизации) и специальное исследование помещения (объекта информатизации).

В зависимости от целей, задач и используемых средств можно выделить следующие виды специальных проверок помещения (объекта информатизации):

– проверка радиоэлектронной аппаратуры, устанавливаемой в помещении;

– проверка помещения на предмет наличия в нем закладных устройств;

– радиомониторинг помещения;

– проверка помещения на предмет наличия в нем скрытых видеокамер;

– визуальный осмотр и специальная проверка новых предметов (подарков, предметов интерьера, бытовых приборов и т. п.) и мебели, размещаемых или устанавливаемых в помещении;

– комплексная проверка помещения.

Контрольные вопросы

1. Что такое специальная проверка помещения (объекта информатизации)?
2. Что такое специальное исследование помещения (объекта информатизации)?
3. Охарактеризуйте визуально-оптический канал утечки информации.
4. Охарактеризуйте канал побочного электромагнитного излучения и наводок.
5. В чем разница между прямым акустическим и виброакустическим каналами утечки информации?
6. В чем разница между оптоэлектронным и акустоэлектрическим каналами утечки информации?
7. В чем разница между прямым акустическим и параметрическим каналами утечки информации?
8. Какие выделяют организационные методы защиты информации от утечки по акустическим каналам?
9. Что может быть отнесено к организационно-техническим методам защиты информации от утечки по техническим каналам?
10. Какие можно выделить виды специальных проверок помещения (объекта информатизации)?

10. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Основная терминология темы. **Фишинг (от англ. phishing – «выуживание идентификаторов»)** – способ получения идентификаторов пользователя информационной системы (логин, пароль, данные платежной карты и т. д.) нарушителем, который основан на предоставлении пользователю такой информации и создании нарушителем таких условий ее восприятия, при которых пользователь примет ошибочное решение и в результате чего выполнит определенное действие, которое является выгодным для нарушителя (передача идентификаторов, загрузка вредоносной программы и т. п.).

Эмоциональное состояние человека – психическое состояние, мотивирующее и регулирующее его деятельность (поведение, восприятие, мышление и т. д.), обусловленное его переживаниями и отношением в данный момент времени к окружающему миру, а также к себе лично.

Методология социальной инженерии. Американский психолог Абрахам Маслоу утверждал, что у человека базовыми потребностями являются: физиологические (удовлетворение голода, необходимость в одежде, необходимость в крове и т. п.) и безопасность. Если эти потребности удовлетворяются, то человек может реализовать свои высшие потребности, одна из которых – общение. У общения всегда есть цель и по своей сути это процесс психологического взаимодействия людей, который заключается в том, что один человек другому передает информацию в некотором виде (рис. 10.1).

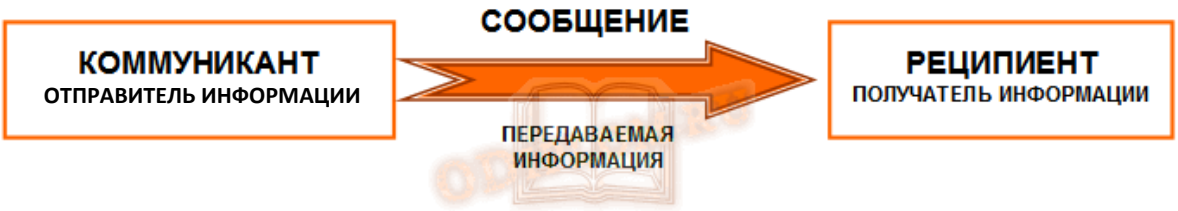


Рис. 10.1. Схематичное изображение процесса передачи информации от одного человека к другому

Процесс восприятия и понимания получаемой информации вторым человеком будет зависеть от жизненного опыта, который он имеет, его отношения к лицу, которое ему передает информацию, и самое важное – от эмоционального состояния человека, воспринимающего информацию.

Выделяют следующие особенности общения людей.

1. **Общение** – это потребность человека, и у этого процесса всегда есть цель, например получение информации или времяпровождение. Хотя можно предположить, что в процессе общения многие люди об этом даже не задумываются.

2. В процессе общения происходит **обмен эмоциями**. Например, полученная человеком информация может его развеселить или, наоборот, расстро-

ить. Эмоции непосредственно **влияют на восприятие информации**. Изменение эмоционального состояния человека приводит, как правило, к снижению способности критически мыслить.

3. В процессе общения происходит **влияние на поведение человека**. Передавая информацию человеку, мы его можем побудить к действию или бездействию.

Содержание и характер взаимодействия людей определяется внутренними побуждениями человека. Обсудим эти побуждения.

1. Потребность – психическое состояние, выражающееся в «дискомфорте», напряжении, неудовлетворенности какого-либо желания. Для того чтобы человек вступил в процесс общения, необходимо, чтобы у него была такая потребность. Чем «сильнее» такая потребность, тем больше вероятность того, что он будет общаться. Если у человека нет желания общаться (нет потребности), то и общаться он не будет.

2. Интерес – эмоциональный процесс, связанный с потребностью человека изучить объект интереса, характеризующийся повышенным вниманием к объекту интереса. Если, как говорят, особого желания общаться нет, то это желание, а по сути потребность, может появиться в случае, если человеку сообщить некоторую интересующую его информацию. Резюмируя, можно заметить следующее: потребность в общении существует у многих людей, но желание общаться появится тогда, когда человеку будет интересно получить некоторые сведения, а интерес к ним будет обусловлен необходимостью получить такие сведения.

3. Мотивация – психофизиологический процесс, управляющий поведением человека, определяющий направленность, организованность и активность его действий. Передавая интересную для человека информацию, можно побудить его выполнить какое-либо действие или не делать что-то.

Рассмотрим пример. Допустим, человек собрался идти в магазин и приобрести некоторый товар. Следуя в магазин, он по пути встречает друга и от него получает информацию о том, что такого товара там уже нет или цена его высока, и такая цена не устраивает этого человека. Исходя из этого, человек может отказаться от того, чтобы пойти в магазин. Так как у него нет потребности проводить время в магазине, смотря на товары не покупая их. Что произошло? Человек отказался идти в магазин, а причиной бездействия стала получение им информации об отсутствии в магазине объекта интереса. А если такую информацию сообщил бы ему не друг, а, скажем, посторонний человек, которого он встретил по пути в магазин? Вполне вероятно, что человек бы не поверил. Посмотрим с другой стороны. А действительно ли друг сообщил достоверную информацию? А вдруг товар был, и друг сообщил ложные сведения, потому что решил сам его купить и таким образом устранил конкурента в лице этого человека? Для уточнения ситуации нужны полные и достоверные сведения.

Таким образом, содержание и характер взаимодействия людей определяется особенностями выполняемых человеком действий, которые можно характеризовать следующим образом:

1. Цель – желаемый результат, на который направлен процесс деятельности человека.

2. Методы – совокупность приемов или операций, используемых для достижения поставленной цели.

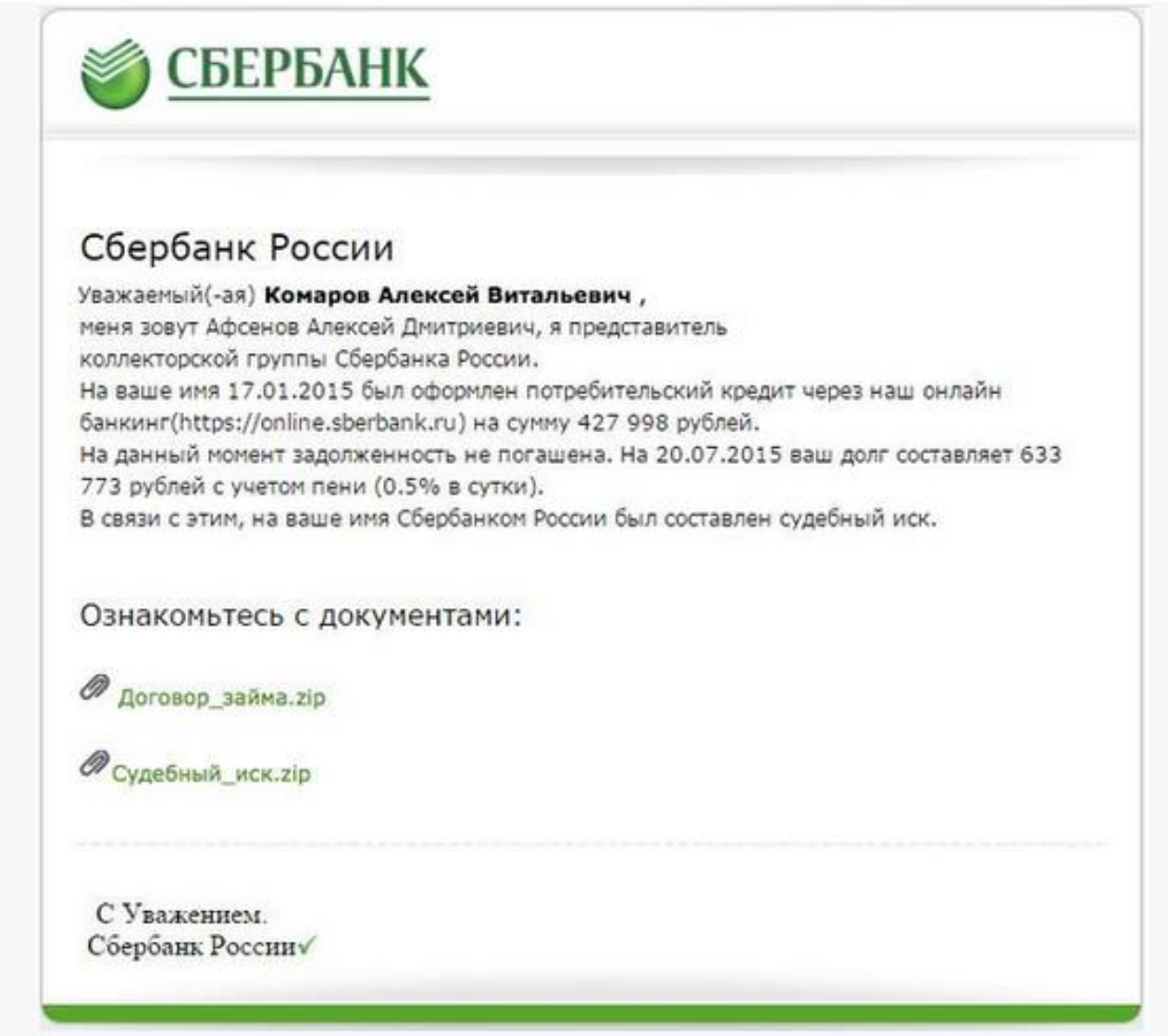
3. Средства – материальные (предметы), энергетические (мышечная энергия) и информационные (речь) образования, используемые при реализации методов.

Исходя из вышеизложенного, необходимо заметить, что эмоциональное состояние человека является психическим состоянием, мотивирующим и регулирующим его деятельность (поведение, восприятие, мышление и т. д.), обусловленное его переживаниями и отношением в данный момент времени к окружающему миру, а также к себе лично. Изменяя эмоциональное состояние человека за счет передачи ему информации, можно управлять действиями человека, причем выполнять он будет действия не по принуждению.

Социальная инженерия – это один из подходов к социальному программированию (манипуляции), целью которого является получение несанкционированного доступа к информации, распространение и (или) предоставление которой ограничено, независимо от формы ее представления. Резонно предположить, что объектами подобного рода манипуляции является(-ются) субъект(-ы), имеющий(-ие) право санкционированного доступа к подобной информации или обладающий(-ие) знаниями о ее содержании. Период начала «цветения» социальной инженерии связан с серединой 1970-х годов. Именно в это время американский тинейджер Кевин Митник, будущий хакер, консультант по информационной безопасности и автор книги «Искусство обмана», ряда других «профильных» книг, воплощал свои затеи по атакам на телефонные компании. В названной книге Кевин поделился знаниями о том, как делать такие и подобные им атаки. Неплохо было бы, конечно, с его стороны издать продолжение под названием «Последствия обмана», так как Митника последствия не обошли стороной. Одно из самых мирных из них было связано с десятилетним запретом на использование телефонов и информационных сетей.

Условия, при которых усиливается социотехническое воздействие на человека. Основным условием для усиления социотехнического воздействия на человека является изменение его эмоционального состояния для того, чтобы ослабить его критическое мышление. Для этого нарушитель может использовать одну из следующих тактик.

1. Передать объекту воздействия сведения о том, что он или кто-то из близких ему людей в опасности. Например, сообщить ему о некоторой существенной для него проблеме и, пока эмоциональное состояние человека не пришло в норму, предложить ему помощь в решении обозначенной нарушителем проблемы (тактика «страха») (рис. 10.2). Суть помощи будет сводиться к завладению нарушителем идентификаторами пользователя. В данном случае на эмоциональное состояние человека воздействует страх. Пока он испуган – им можно управлять. Это классика фишинга, так как бесстрашных людей не бывает. Нарушитель в данном случае использует потребность человека в безопасности.


СБЕРБАНК

Сбербанк России

Уважаемый(-ая) **Комаров Алексей Витальевич** ,
меня зовут Афсенов Алексей Дмитриевич, я представитель
коллекторской группы Сбербанка России.
На ваше имя 17.01.2015 был оформлен потребительский кредит через наш онлайн
банкинг(https://online.sberbank.ru) на сумму 427 998 рублей.
На данный момент задолженность не погашена. На 20.07.2015 ваш долг составляет 633
773 рублей с учетом пени (0.5% в сутки).
В связи с этим, на ваше имя Сбербанком России был составлен судебный иск.

Ознакомьтесь с документами:

Договор_займа.zip

Судебный_иск.zip

С Уважением.
Сбербанк России

Рис. 10.2. Целенаправленное фишинговое почтовое сообщение с вложенными файлами

2. Сообщить человеку о радостной для него новости, например, что он выиграл крупную денежную сумму и может ее получить, но для этого необходимо, чтобы он сообщил идентификаторы своей банковской карты или оплатил перевод «выигранных» денежных средств (рис. 10.3) (тактика «радости»). Получение внезапного подарка или приза всегда влияет на эмоциональное состояние человека, а также притупляет его критическое мышление. Подобная тактика является самой «древней» и носит наименование «нигерийских писем». В данном случае воздействие происходит на физиологические потребности человека, которые удовлетворяются за счет денежных средств. А внезапный выигрыш как раз и мотивирует его забрать. Нарушитель таким образом воздействует на физиологические потребности человека, так как они могут быть удовлетворены за счет денежных средств.

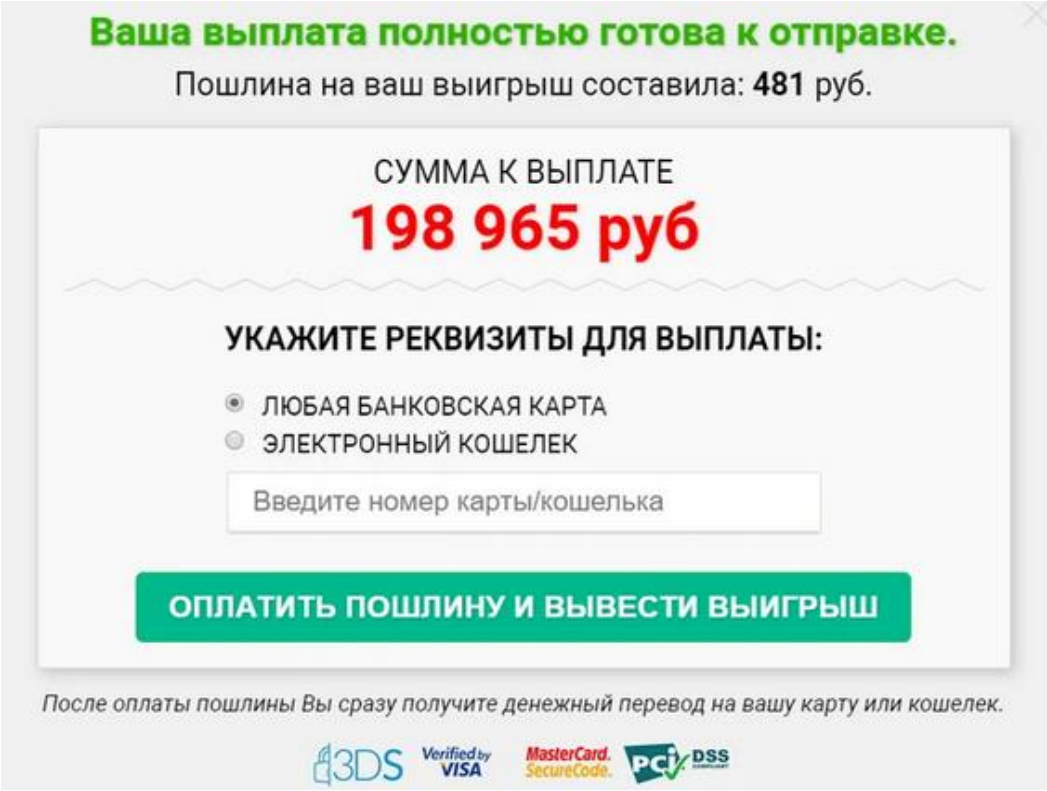


Рис. 10.3. Фишинговое почтовое сообщение о выигрыше

3. Послать сообщение пользователю электронной почты с некоторой интересной темой в надежде на его любопытство (тактика «любопытства»). Любознательность человека является мишенью для эффективной реализации почтового фишинга. Грамотный выбор легенды сообщения (рис. 10.4) и массовая его рассылка могут дать возможность нарушителю скомпрометировать множество идентификаторов. В данном случае человеком движет потребность в познании нового, что и использует нарушитель.

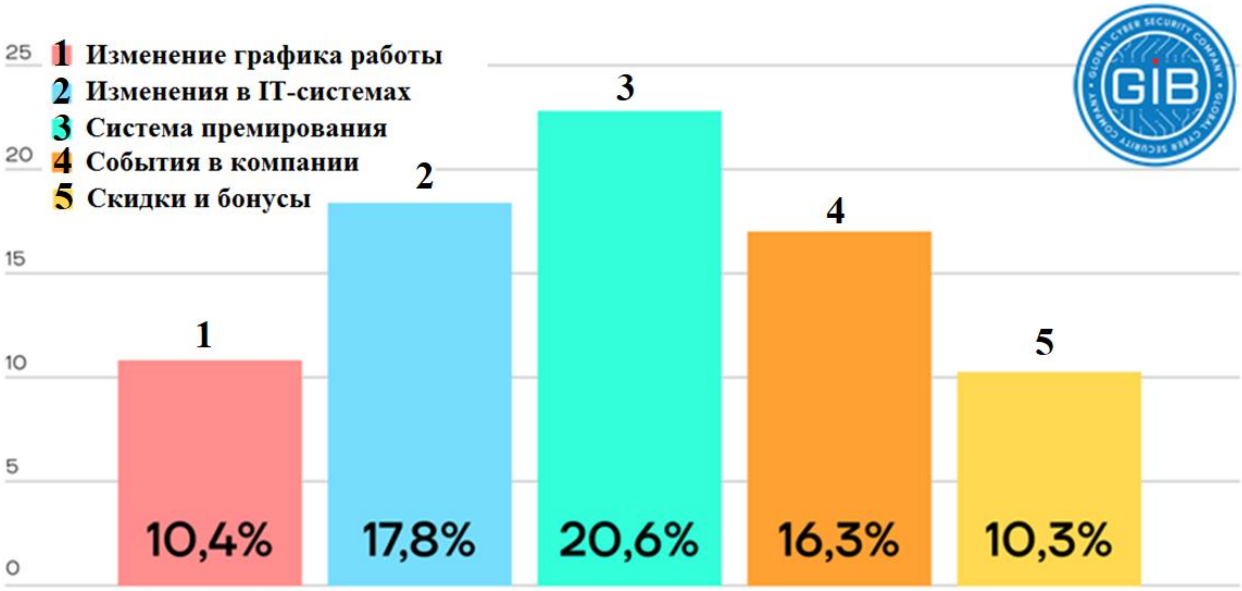


Рис. 10.4. Средняя результативность легенд сообщений электронной почты

Методология противодействия социотехническим воздействиям.

Фишинг. Во многих организациях мира в основе обеспечения бизнес-процессов лежит применение электронной почты, которая позволяет передавать не только текстовые сообщения, но и различные файлы. Проверка подлинности сообщения, переданного по электронной почте на широко используемых почтовых ресурсах в корпоративных и глобальных информационных сетях, затруднительна. Для обеспечения безопасности информации, которая принимается, передается, обрабатывается и хранится в информационных системах, используются средства защиты информации, которые ограничивают к ней доступ посредством парольной защиты. Такое положение дел в информационных системах обуславливает проблему фишинга.

Фишинг ориентирован на введение в заблуждение пользователя информационной системы, но его критическое мышление является барьером при принятии им ошибочного решения. Поэтому, понимая, что в уравновешенном эмоциональном состоянии пользователь не может совершить необходимые для нарушителя действия, нарушитель обязан изменить его эмоциональное состояние таким образом, чтобы нейтрализовать его критическое мышление на то время, когда он будет совершать выгодное для нарушителя действие. В этом заключается сущность социальной инженерии как методе управления действиями пользователя информационной системы.

Фишинг делится на пять видов.

1. Фишинговое письмо с прикрепленным вложением. В качестве вложения используется файл (рис. 10.5), содержащий вредоносную программу. Для того чтобы обойти средства антивирусной защиты, которые могут функционировать на периметре информационной сети, файл упаковывают, например используя архив *.zip или *.rar, и доступ к файлу в архиве блокируется паролем, который передают в тексте письма. Этот вид фишинга приводит к несанкционированному доступу нарушителя к информационной системе, в результате которого могут произойти следующие события:

– выгрузка данных с устройства пользователя и при определенных условиях из информационной системы, к которой его устройство подключено;

– получение всех идентификаторов пользователя к его учетным записям, которые он использует на данном устройстве;

– запуск вредоносной программы-шифровальщика для получения выкупа за расшифрование информации на данном устройстве.

Вместе с тем если на устройстве пользователя установлено средство антивирусной защиты и у этого средства есть сигнатуры для обнаружения вредоносной программы, то, когда пользователь разархивирует файл, средство защиты может обнаружить вредоносную программу.

Рис. 10.5. Фишинговое почтовое сообщение с вложенным файлом

2. Фишинговое письмо с активной ссылкой. В таком письме отсутствует прикрепленный файл с вредоносной программой, а присутствует ссылка на этот файл, который находится на сервере за пределами информационной системы, к которой имеет доступ пользователь. Переход по ссылке будет инициализировать соединение с сервером от имени пользователя и загрузку файла с вредоносной программой (рис. 10.6).

3. Фишинговое письмо с активной ссылкой для перенаправления пользователя на сторонний сервер. Этот вид фишинга позволяет нарушителю в случае перехода пользователя по активной в письме ссылке перенаправить его на сервер, который он контролирует, например для сбора идентификаторов пользователя (рис. 10.7).

4. Фишинг, основанный на использовании IP-телефонии. Для этого нарушитель использует средства IP-телефонии (IP – Internet Protocol), например Viber. Такой вид фишинга часто называют вишингом. Речевая коммуникация нарушителя с пользователем может дать возможность нарушителю получить идентификаторы пользователя или мотивировать пользователя установить себе на устройство вредоносную программу.

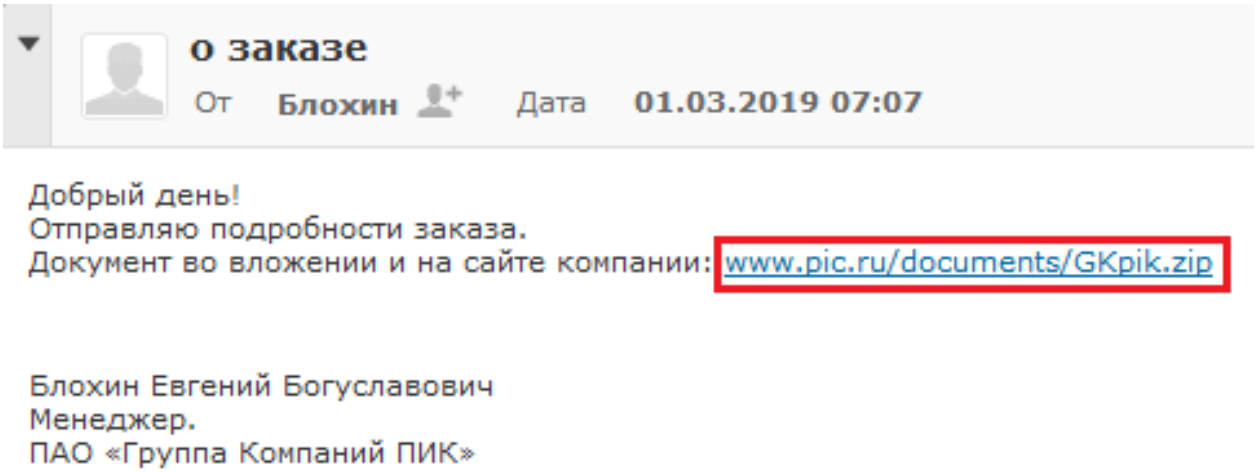


Рис. 10.6. Фишинговое почтовое сообщение с активной ссылкой

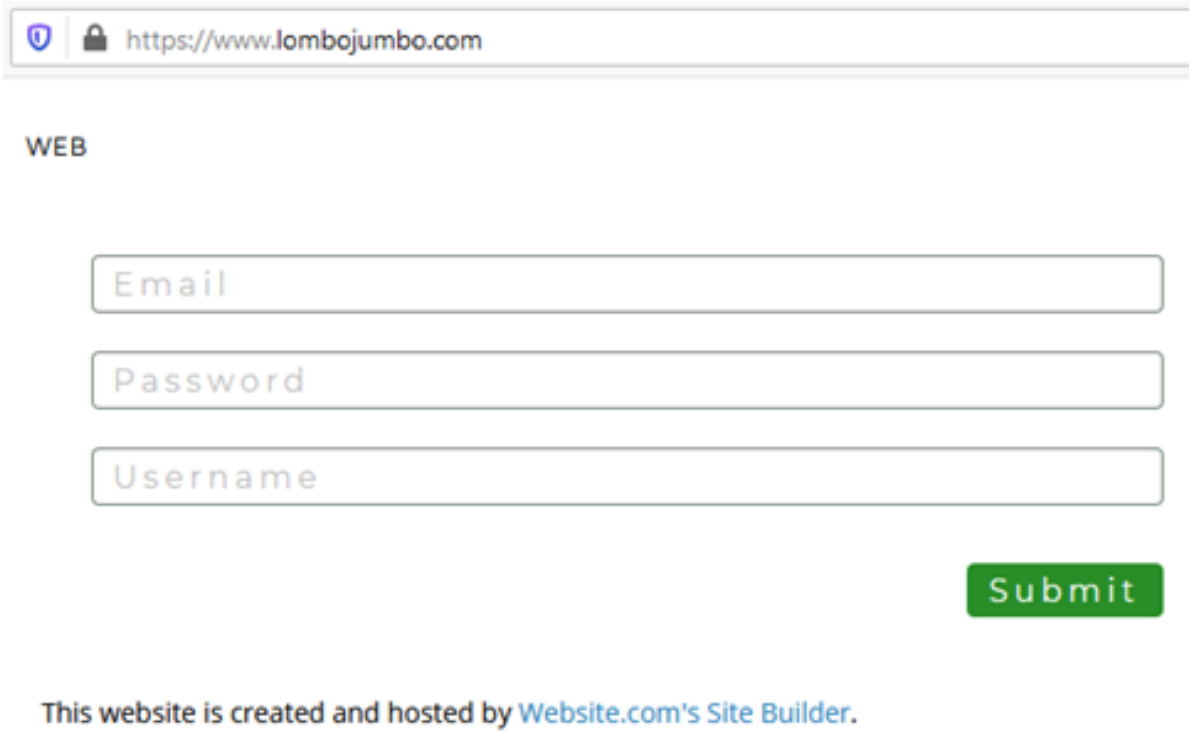


Рис. 10.7. Внешний вид фишингового сайта для сбора идентификаторов электронной почты

Вишинг часто используется мошенниками для того, чтобы получить доступ к денежным средствам человека. Выполним анализ изображения, представленного на рис. 10.8. Абоненту банка поступает входящий вызов. В данном случае для коммуникации используется IP-телефония и приложение Viber.

Этот входящий вызов осуществляется мошенниками, потому что сотрудники банков не используют подобного рода приложения для коммуникации с клиентами банка. Многие люди об этом знают, но в суматохе внимательность человека снижается, и поэтому мошенник, вступив в речевую коммуникацию,

может убедить человека, что является сотрудником банка, и обманным путем (манипулируя человеком) побудить его выполнить выгодные для мошенника действия.

Вместе с тем мошенник учитывает способы восприятия информации человеком. Первое, на что обращают, как правило, внимание клиенты банка – это логотип банка, и здесь он соответствует действительности. Второе – наименование банка. Оно не совсем корректно указано: слово «Банк» выделено с большой буквы, но это сделано намеренно, что позволяет клиенту обеспечить на уровне его подсознания верную ассоциацию логотип – банк. Вместе с тем на данном рисунке можно рассмотреть еще одну деталь, которая указывает на то, что этот входящий вызов не относится ни к одному из известных банков Республики Беларусь – это международный код в номере телефона. Первые три цифры идентифицируют страну и 372 – это Эстония.

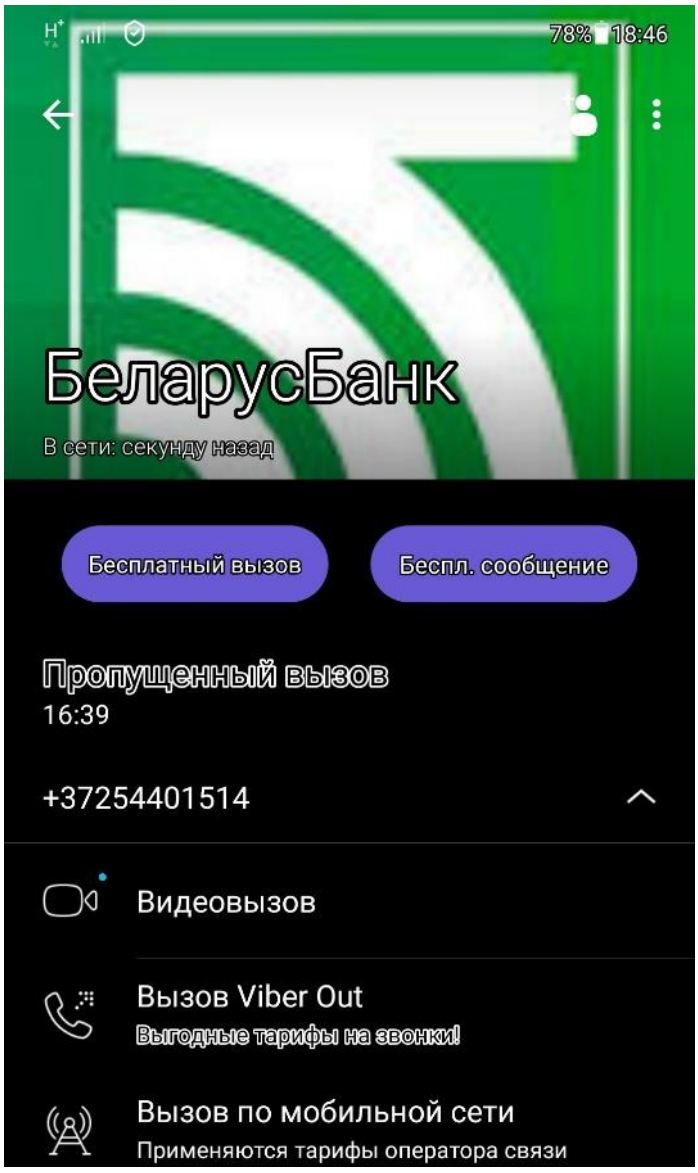


Рис. 10.8. Внешний вид мессенджера Viber, используемого нарушителем

5. Целенаправленный фишинг (спиарфишинг, от англ. spear – «гарпун») – сообщения, которые формирует нарушитель, передаются посредством электронной почты. Их текст адресован конкретному человеку, так как нарушитель до составления такого сообщения смог получить доступ к персональным данным этого человека.

Рассмотрим признаки фишинга, которые можно обнаружить при анализе сообщений электронной почты. К ним мы будем относить отклонение от нормального положения дел. Таким образом, суть анализа сообщений – это обнаружение аномалий.

1. *Отправитель сообщения и время его отправления*. Отправитель может быть известный или неизвестный (известных отправителей сложнее игнорировать). Время отправления сообщения может быть рабочее или нерабочее (деловая переписка в нерабочее время может быть аномалией, так как многие люди редко задерживаются на работе для выполнения своих должностных обязанностей, откладывая на завтра то, что не сделали сегодня).

2. *Почтовый адрес отправителя сообщения*. Необходимо обратить внимание на домен и наименование почтового ящика. Возможные аномалии: в результате анализа содержания сообщения делается вывод, что речь идет о деловой переписке, а для отправки сообщения используется не корпоративный домен электронной почты, а другие распространенные домены (например, mail.ru, gmail.com и т. д.). Наименование ящика электронной почты не содержит фамилии или имени отправителя сообщения (наличие фамилии, имени или инициалов в наименовании ящика – частый случай для корпоративной почты). Проверка принадлежности домена (наименование ящика после символа «@») может быть реализована путем его введения в адресную строку браузера. Это позволяет понять, какая электронная почта использовалась при отправке сообщения.

3. *Текст сообщения и его оформление, тема сообщения.* Текст сообщения должен отвечать требованиям деловой переписки не только по содержанию, но и оформлению. Признаки деловой переписки:

– приветственное обращение по имени и отчеству к адресату;

– Ф. И. О. отправителя, его должность и некоторые реквизиты организации.

4. *Тип вложения.* Возможные аномалии:

– вложение является архивом (*.rar, *.zip);

– вложение – гипертекстовая ссылка;

– вложение имеет неизвестное расширение (*.001) или двойное расширение (*.docx.exe).

5. *Наименование вложения.* Возможная аномалия: наименование файла представляет собой написание русского слова в транслитерации (Oplata.zip, Dokumenti_dlia_proverki.001).

Используя признаки фишинга, выполним анализ сообщения электронной почты (рис. 10.9) и определим признаки фишинга. Исходные данные для анализа сообщения:

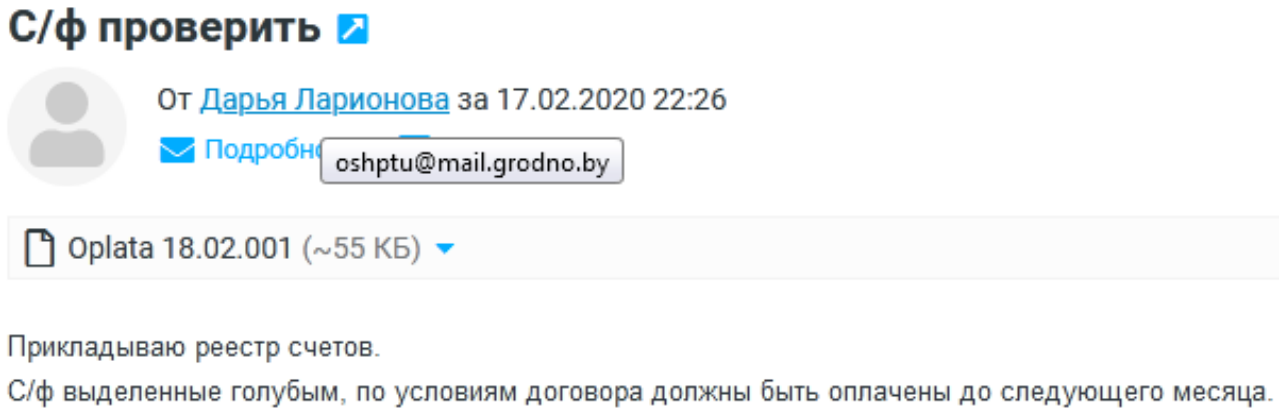


Рис. 10.9. Сообщение электронной почты

1. Сообщение получено преподавателем БГУИР на его корпоративную электронную почту.

2. Университет имеет корпоративную почту в домене bsuir.by.

1. Отправитель сообщения и время его отправления. Сообщение пришло от неизвестного для преподавателя лица. Время отправки – нерабочее, хотя, судя по тексту сообщения, речь идет о деловой переписке.

Так как сообщение пришло не по назначению, то в данном случае нарушителем используется тактика «любопытства». Если такое сообщение было бы доставлено сотруднику бухгалтерии, тогда бы была тактика «страха», ввиду того, что несвоевременная оплата счетов ведет к проблемам у человека, не выполнившего такую должностную обязанность. Это умозаключение подтверждается содержанием сообщения, поэтому его текст имеет эмоциональную окраску, побуждающую получателя к действию.

2. Почтовый адрес отправителя сообщения. Почтовый адрес отправителя сообщения: «oshptu@mail.grodno.by». Наименование почтового ящика «oshptu» не имеет ничего общего с его отправителем – «Дарьей Ларионовой». Домен, с которого отправлено письмо, «mail.grodno.by» не имеет отношения к корпоративной почте конкретной организации. Этот сервис электронной почты предоставляется РУП «Белтелеком», что подтверждается проверкой домена.

3. Текст сообщения и его оформление, тема сообщения. Текст сообщения имеет признаки деловой переписки, хотя в оформлении отсутствуют такие признаки. Тема письма «С/ф проверить» означает, что сообщение используется для пересылки счета-фактуры (сокращение «С/ф»). Преподаватель университета не является сотрудником бухгалтерии, поэтому счетами-фактурами он не занимается. Исходя из чего, можно сделать вывод, что письмо пришло не по назначению. Кроме того, необходимо учесть, что случайностью пересылку сведений, относящихся к информации, распространение и (или) предоставление которой ограничено (счет-фактура), назвать сложно. Признаки управления действиями получателя сообщения присутствуют. Они реализуются через осмысление текста сообщения. Так, например, для того чтобы оплатить счет-фактуру

или для того чтобы полюбопытствовать, что находится в содержании счета-фактуры, нужно открыть файл.

4. Тип вложения. К письму прикреплен файл, который имеет неизвестное расширение *.001, хотя речь идет о счете-фактуре, соответственно расширение файла должно соответствовать документам данной категории.

5. Наименование вложения. Вложением является файл с русским наименованием, написанным в транслитерации «Oplata 18.02».

Вывод: данное сообщение является фишинговым. Открытие файла приведет к запуску и установке вредоносной программы. Сообщение необходимо удалить.

Контрольные вопросы

1. На чем основан фишинг?
2. Что такое потребность?
3. Что такое интерес?
4. Что такое мотивация?
5. В чем заключается сущность социальной инженерии?
6. Какие выделяют виды фишинга?
7. Какой из видов фишинга наиболее опасный? Обоснуйте ответ.
8. Какой из видов фишинга наиболее эффективный для нарушителя? Обоснуйте ответ.
9. Какой из признаков обнаружения фишинговых сообщений наиболее оптимальный? Обоснуйте ответ.
10. Какие этапы включает в себя алгоритм анализа сообщений электронной почты на предмет того, являются ли эти сообщения фишинговыми?

11. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Основная терминология темы. **Информационная система** – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств.

Информационная технология – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации.

Информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах.

Информатизация – организационный, социально-экономический и научно-технический процесс, обеспечивающий условия для формирования и использования информационных ресурсов и реализации информационных отношений.

Информационные отношения – отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий.

На рис. 11.1 представлена схема, которая демонстрирует отношения между объектами, обозначаемыми с помощью рассмотренных терминов.

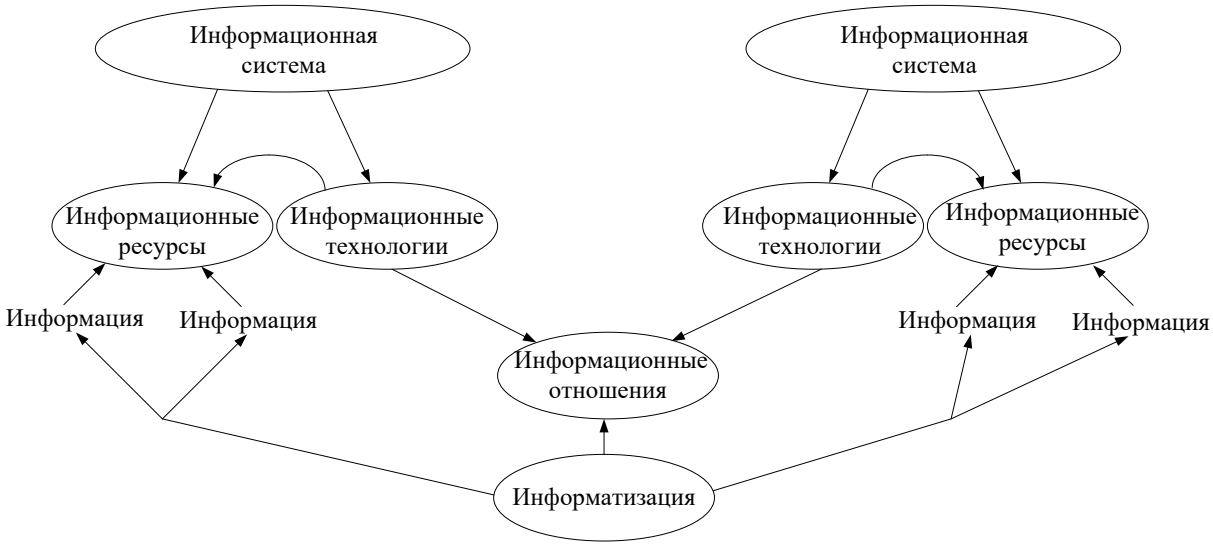


Рис. 11.1. Схема, демонстрирующая взаимосвязь между рассмотренными терминами

Очевидно, что в информационных системах может содержаться информация, распространение и (или) предоставление которой ограничено. В связи с этим такие системы должны быть защищенными, т. е. в их рамках должны реализовываться процессы не только поиска, получения, передачи, сбора, обработ-

ки, накопления, хранения, распространения и (или) предоставления, но и защиты информации.

Архитектура информационной системы. Все элементы информационной системы можно условно разделить на две группы: пассивные и активные. Элементы, относящиеся к первой группе, называют объектами системы, элементы, относящиеся ко второй группе, – субъектами системы.

Таким образом, применительно к информационной системе объект – это компонент, хранящий, принимающий или передающий информацию. В свою очередь, субъект – это компонент информационной системы, который может явиться причиной потока информации от объекта к объекту или изменения состояния системы.

Следовательно, информационный ресурс – это объект информационной системы, а пользователи системы – это ее субъекты.

Направления обеспечения защиты информации в информационных системах. Выделяют следующие направления обеспечения защиты информации в информационных системах:

– идентификация и аутентификация пользователей;

– управление доступом;

– криптографическая защита информации.

Эти подходы в своей совокупности формируют основу политики безопасности для большинства используемых в настоящее время информационных систем. Под политикой безопасности информационной системы следует понимать набор законов, правил и практических рекомендаций, на основе которых обеспечивается защита информации в этой системе.

Идентификация и аутентификация пользователей информационных систем. Под идентификацией следует понимать процесс присвоения уникального признака субъекту (объекту) информационной системы, по которому он будет опознаваться в рамках этой системы. Соответственно, уникальный признак, который присваивается субъекту информационной системы в ходе процедуры регистрации и который предоставляется этим субъектом в ходе процедуры аутентификации, называется идентификатором субъекта. Процедура аутентификации, в свою очередь, представляет собой проверку подлинности идентификатора субъекта (объекта) информационной системы.

Субъектами информационной системы, относящимися к категории ее пользователей, в настоящее время применяются следующие идентификаторы:

– пароль;

– устройство аутентификации;

– биометрический(-ие) признак(-и).

Под паролем следует понимать отличительную характеристику пользователя информационной системы, представляющую собой секретную информацию, распространение которой запрещено в соответствии с требованиями политики безопасности указанной системы.

Выделяют следующие формы представления пароля:

– ключевое слово;

– комбинация цифр для открытия кодового замка;

– комбинация символов, предназначенных для введения с клавиатуры.

Под устройством аутентификации следует понимать некоторый уникальный предмет, находящийся у субъекта и являющийся его отличительной характеристикой.

Выделяют следующие типы устройств аутентификации:

– Smart-карта (рис. 11.2, *а*);

– USB-брелок (рис. 11.2, *б*);

– OTP-токен (от англ. One-Time Password) – рис. 11.2, *в*.

Внешний вид устройств аутентификации каждого из указанных типов представлен на рис. 11.2.

а *б* *в*

Рис. 11.2. Внешний вид устройств аутентификации:
а – Smart-карта; *б* – USB-брелок; *в* – OTP-токен

Пароли и устройства аутентификации как идентификаторы пользователей информационных систем характеризуются рядом недостатков. В частности, пароль может быть забыт пользователем (особенно в тех случаях, когда в рамках политики безопасности информационной системы предусмотрены требования его частой смены и соответствия определенным критериями) или, в случае если этот пароль не меняется в течение длительного промежутка времени, он может быть скомпрометирован нарушителем безопасности информационной системы.

Устройства аутентификации не характеризуются указанными недостатками, однако им присущ ряд других, которые условно принято обозначать следующим образом:

– халатность пользователя типа 1;

– халатность пользователя типа 2.

Халатностью пользователя типа 1 называют такие его действия, которые приводят к тому, что устройство аутентификации оказывается оставленным в рабочей станции. Халатности пользователя типа 2 соответствуют действия, в результате совершения которых устройство аутентификации оказывается утерянным.

На помощь в борьбе с описанными «недугами» может прийти введение ряда организационных мер. В частности, нераспространению халатности пользователя типа 1 благоприятствуют следующие меры:

– заставить пользователя носить с собой устройство аутентификации (например, объединив его с ключом от электронного замка, установленного на

входной двери в рабочий кабинет пользователя или комнату отдыха предприятия (если оная имеется));

– настроить рабочую станцию пользователя таким образом, чтобы выполнялись блокировка доступа к ней в случае фиксирования факта бездействия пользователя в течение определенного промежутка времени (3–5 минут) и запрос повторной аутентификации для разблокировки доступа.

Для того чтобы снизить степень риска, которому может быть подвержена информационная система в результате халатности пользователя типа 1, рациональным представляется введение следующих мер:

– защита PIN (Personal Identification Number) устройства аутентификации от перебора;

– увеличение объема времени, затрачиваемого на проверку корректности введенного PIN устройства аутентификации (введение так называемой задержки на аутентификацию).

Очевидно, что все описанные меры должны быть представлены в политике безопасности информационной системы.

Все рассмотренные недостатки не характерны для биометрических характеристик как идентификаторов.

Биометрической характеристикой называют измеримую поведенческую или физиологическую черту живого человека.

Поведенческие биометрические характеристики включают в себя совокупность данных, которые могут быть получены на основе результатов анализа действий человека (особенности походки, динамика клавиатурного почерка, динамика рукописной подписи и т. п.).

Физиологические биометрические характеристики включают в себя данные, которые могут быть получены на основе измерения анатомических характеристик человека (отпечаток пальца, рисунок радужной оболочки глаза, рисунок вен на руке, геометрия лица, параметры голоса и т. п.).

Биометрические характеристики также принято разделять на статические и динамические. Резонно предположить, что биометрическая характеристика является статической в случае, если ее параметры не зависят от возраста, настроения и состояния здоровья человека, от внешних факторов. Параметры динамической биометрической характеристики, наоборот, подвержены влиянию указанных и ряда других факторов. Следует отметить, что все поведенческие биометрические характеристики являются динамическими, но не все физиологические биометрические характеристики являются статическими. Например, параметры голоса весьма зависят от настроения человека и состояния его здоровья. Именно поэтому информационные системы, в рамках которых реализуются механизмы аутентификации, основанные на анализе параметров голоса, следует более длительно «обучать», чем системы, в рамках которых реализуются альтернативные механизмы аутентификации.

Для того чтобы повысить защищенность информации в информационной системе, механизмы аутентификации в рамках этой системы необходимо реализовывать в соответствии со следующими принципами:

– использование нескольких факторов (например, пароль и динамика клавиатурного почерка, параметры голоса и отпечаток пальца и т. п.), в результате чего аутентификация становится многофакторной;

– запрос ре-аутентификации (повторной аутентификации) пользователя перед выполнением критических изменений (например, сохранение измененных настроек безопасности).

Управление доступом в информационных системах. Выделяют три разновидности моделей управления доступом в информационных системах:

– дискреционная (избирательная) – модель Харрисона – Руззо – Ульмана;

– ролевая (является развитием дискреционной модели);

– мандатная (полномочная) – модель Белла – ЛаПадулы.

Рассмотрим описание каждой из указанных моделей, но прежде отметим, что под термином «модель управления доступом» следует понимать совокупность следующих сведений:

– порядок установления субъектов информационной системы, которые являются владельцами ее объектов;

– порядок разграничения доступа субъектов информационной системы к ее объектам;

– перечень прав субъектов информационной системы по отношению к ее объектам.

В табл. 11.1 кратко представлены указанные сведения, соответствующие каждой из моделей управления доступом. В целях оптимизации размера таблицы эти сведения соответственно обозначены с помощью следующих словосочетаний:

– порядок установления владельцев объектов;

– порядок разграничения доступа к объектам;

– перечень прав субъектов.

Таблица 11.1

Характеристики моделей управления доступом

<table>
<tr><th>Наименование модели управления доступом</th><th>Порядок установления владельцев объектов</th><th>Порядок разграничения доступа к объектам</th><th>Перечень прав субъектов</th></tr>
<tr><td>Дискреционная</td><td rowspan="3">Субъект, который создал объект является его владельцем</td><td>На основе матрицы доступа</td><td rowspan="3">Чтение, запись, выполнение</td></tr>
<tr><td>Ролевая</td><td>Присвоение каждому субъекту системы определенной роли</td></tr>
<tr><td>Мандатная</td><td>Присвоение каждому объекту системы определенной метки критичности,
а субъекту системы – уровня прозрачности</td></tr>
</table>

Следует отметить, что в рамках каждой модели управления доступом предполагается, что все объекты и субъекты информационной системы идентифицированы, т. е. характеризуются наличием идентификатора (атрибута, который отличает этот объект (субъект) от других объектов (субъектов) информационной системы).

Разберем более детально порядок разграничения доступа к объектам, соответствующий каждой из моделей управления доступом.

В соответствии с представленной выше таблицей порядок разграничения доступа к объектам, соответствующий дискреционной модели управления доступом, основан на использовании матрицы доступа. По своей сути матрица доступа представляет собой таблицу, в заголовках строк которой указаны идентификаторы объектов информационной системы, а в заголовках столбцов – идентификаторы субъектов информационной системы. На пересечении каждых строки и столбца таблицы (в ее ячейках) представлены сведения о перечне прав (типе доступа) субъекта, идентификатор которого указан в заголовке столбца, по отношению к объекту, идентификатор которого указан в заголовке строки. Схематическое изображение матрицы доступа представлено на рис. 11.3 (использованное на изображении обозначение RO соответствует словосочетанию Read Only («Только чтение»), а обозначение RW – словосочетанию Read and Write («Чтение и запись»)).

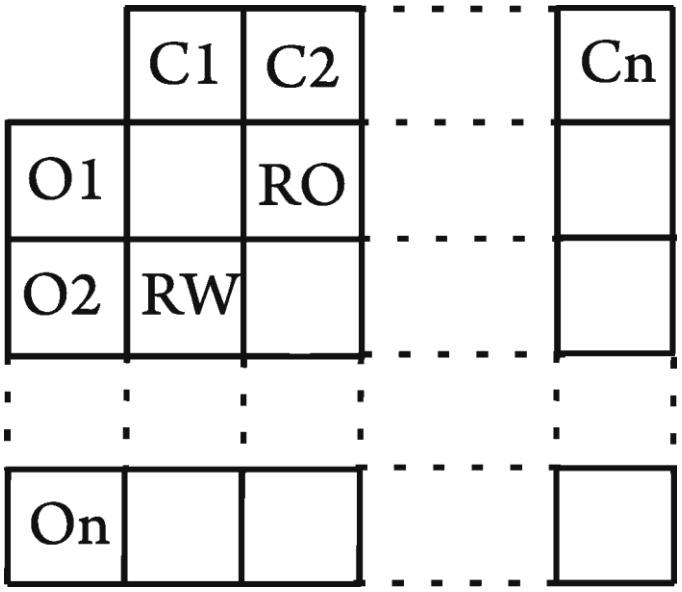


Рис. 11.3. Схематическое изображение матрицы доступа

В рамках описания порядка разграничения доступа к объектам, соответствующего дискреционной модели управления доступом, часто встречаются такие термины, как «профиль», «список доступа» и «мандат».

В данном контексте под профилем следует понимать список объектов информационной системы и прав доступа к ним, ассоциированный с каждым субъектом указанной системы. Иными словами, совокупность сведений, содержащихся в строках матрицы доступа, – это профиль.

Под списком доступа следует понимать список субъектов информационной системы и прав доступа этих субъектов по отношению к объектам указанной системы. Иными словами, совокупность сведений, содержащихся в столбцах матрицы доступа, – это список доступа.

Уверены, что читатель неоднократно встречал окно, скриншот которого представлен на рис. 11.4 (вернее, часть этого окна, ассоциированную со вкладкой «Безопасность»).

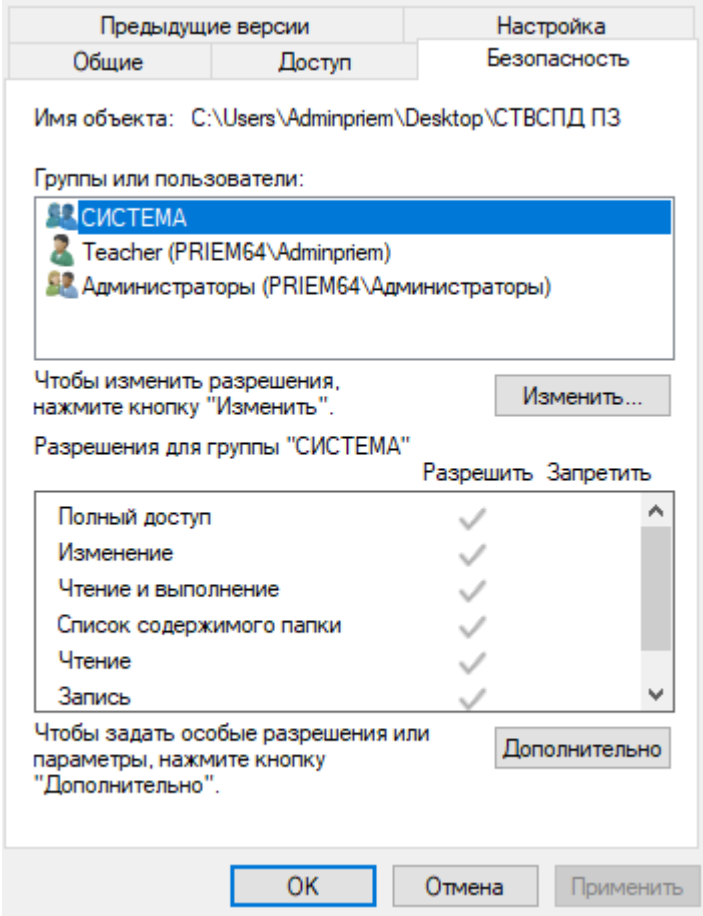


Рис. 11.4. Скриншот диалогового окна для настройки свойств директории

Представленное на рис. 11.4 окно (а вернее, его часть, ассоциированная со вкладкой «Безопасность») содержит не что иное, как список доступа. В связи с этим нетрудно догадаться, что дискреционная модель управления доступом может быть использована в информационных системах, в рамках которых развернута операционная система семейства Windows.

В рамках описания порядка разграничения доступа к объектам, соответствующего дискреционной модели управления доступом, под мандатом следует понимать тип доступа определенного субъекта информационной системы к определенному объекту указанной системы. Иными словами, совокупность сведений, содержащихся в ячейке матрицы доступа, – это мандат.

Порядок разграничения доступа к объектам, соответствующий ролевой модели управления доступом, основан на создании в рамках информационной

системы ролей. В рамках описания порядка разграничения доступа к объектам, соответствующего ролевой модели управления доступом, под ролью следует понимать совокупность разрешений, а под совокупностью разрешений, в свою очередь, следует понимать сведения о типах доступа к определенным объектам (к группе объектов) информационной системы. Роли характеризуются следующими особенностями:

– одна роль может иметь несколько разрешений;

– одно разрешение может принадлежать нескольким ролям.

Каждому из субъектов информационной системы присваивается роль. Особенности присвоения роли следующие:

– один субъект может иметь несколько ролей;

– одну роль могут иметь несколько субъектов.

На рис. 11.5 представлен пример схемы, демонстрирующей особенности разграничения доступа к объектам, соответствующего ролевой модели управления доступом (использованное на изображении обозначение E соответствует слову Execution («Выполнение»)).

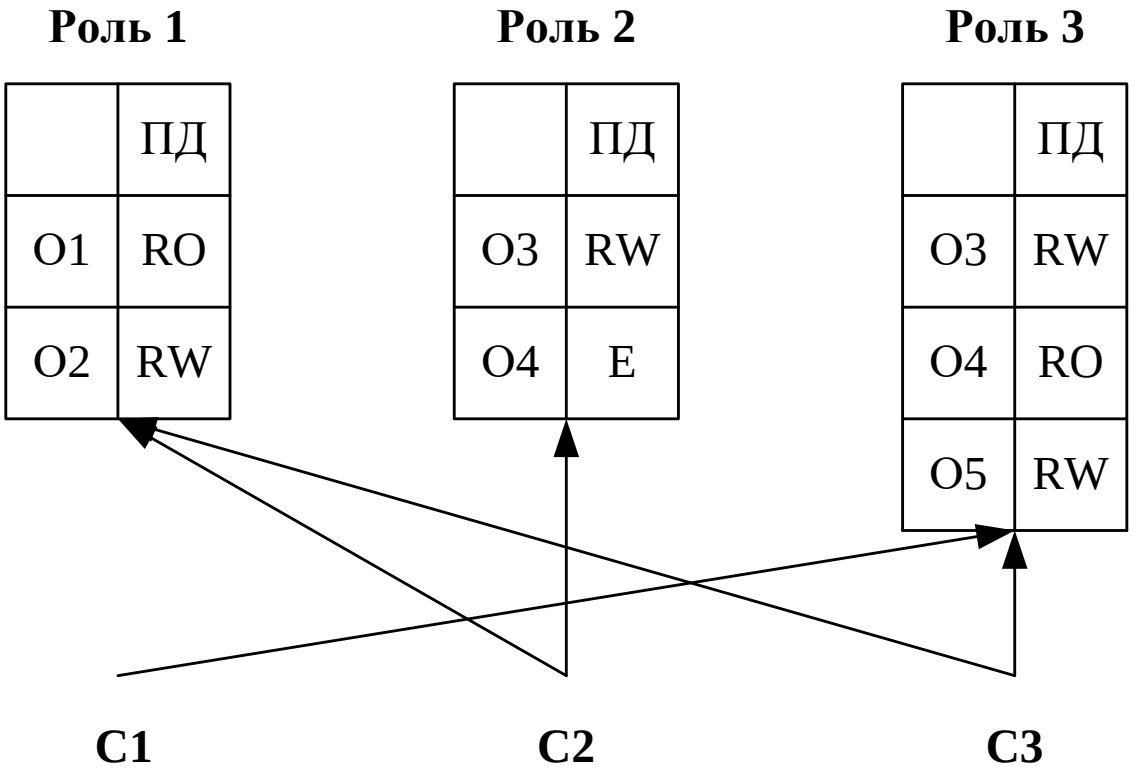


Рис. 11.5. Пример схемы, демонстрирующей особенности разграничения доступа к объектам и соответствующей ролевой модели управления доступом

Так как ролевая модель управления доступом является развитием дискреционной модели управления доступом, то пример условной матрицы доступа, соответствующей этой модели и коррелирующей с вышепредставленной схемой, выглядит так, как представлено на рис. 11.6.

	C1	C2	C3
Роль 1	Запрещена	Разрешена	Разрешена
Роль 2	Запрещена	Разрешена	Запрещена
Роль 3	Разрешена	Запрещена	Разрешена

Рис. 11.6. Пример условной матрицы доступа, соответствующей ролевой модели

И наконец, рассмотрим порядок разграничения доступа к объектам, соответствующий мандатной модели управления доступом. Из табл. 11.1 следует, что этот порядок основан на использовании меток критичности (Security Label, SL), уровней прозрачности (Security Clearance, SC). Метка критичности, как было определено в табл. 11.1, присваивается каждому из объектов информационной системы. Она соответствует ценности содержащейся в нем информации. Уровень прозрачности присваивается каждому из субъектов информационной системы и соответствует максимальному значению метки критичности объектов, к которым субъект имеет права доступа.

Метка критичности и уровень прозрачности могут принимать одно из следующих значений:

– совершенно секретно (Top-secret);

– секретно (Secret);

– критической важности (Confidential);

– не классифицировано (Unclassified).

В англоязычных литературных источниках эти значения называют уровнем безопасности – security level (см., например, Henk C. A. van Tilborg and Sushil Jajodia. Encyclopedia of Cryptography and Security, 2nd Ed. Springer, 2011).

Особенность чтения содержимого объектов информационной системы, соответствующая мандатной модели управления доступом, описывается следующим образом: субъект информационной системы может читать содержимое какого-либо объекта указанной системы в том случае, если уровень безопасно-

сти его SC больше или равен уровню безопасности SL этого объекта, а также если этот субъект имеет право чтения содержимого этого объекта.

Указанная особенность кратко описывается фразой: No Read up Rule.

Особенность изменения содержимого объектов информационной системы, соответствующая мандатной модели управления доступом, описывается следующим образом: субъект информационной системы может изменять содержимое какого-либо объекта указанной системы в том случае, если уровень безопасности его SC равен уровню безопасности SL этого объекта, а также если этот субъект имеет право изменения содержимого этого объекта.

Указанная особенность кратко описывается фразой: No Write Down Rule.

Модель управления доступом, применяемая в рамках информационной системы, определяет особенности реализации процедуры авторизации в рамках этой системы. Авторизация представляет собой процедуру проверки прав доступа субъекта информационной системы к ее объекту.

Элементы аппаратного и программного обеспечения информационной системы, выполняющие в ее рамках функции идентификации, аутентификации и авторизации, должны быть проверены на предмет корректности функционирования и защищены от модификации. Такие элементы принято называть ядром безопасности информационной системы (Security Kernel).

Ядро безопасности информационной системы является основой ее достоверной вычислительной базы (Trusted Computing Base). Достоверная вычислительная база – это полностью защищенный механизм информационной системы (включая аппаратные и программные средства), отвечающий за поддержку реализации ее политики безопасности.

Следует также отметить, что ядро безопасности информационной системы является основой для реализации концепции механизма ее защиты. Эта концепция носит название «монитор ссылок» (Reference Monitor).

Если управление доступом в информационной системе построено на одной из рассмотренных моделей, то оно является логическим. Альтернативой логическому управлению доступом в информационной системе являются физическое, временное и криптографическое.

Физическое управление доступом заключается в создании условий, при которых снижается вероятность проникновения нарушителя безопасности информационной системы в помещения, где располагаются ее технические средства.

Временное управление доступом заключается в создании условий, при которых использование объектов информационной системы представляется возможным для ее субъектов в случае, если соблюдаются определенные временные условия (например, день, когда субъект может использовать объект, не должен быть выходным днем или промежуток времени, в течение которого субъект может использовать объект, не должен превышать получаса и т. п.) [16–19].

Уязвимости информационных систем. Уязвимости информационных систем обусловлены уязвимостями программных и программно-технических средств, входящих в состав этих систем.

Для получения информации об актуальных уязвимостях программных средств следует обращаться к базе данных CVE (Common Vulnerabilities and Exposures). Каждая запись в этой базе представляет собой совокупность полей, в каждом из которых содержится одно из нижеследующего:

– идентификатор уязвимости;

– описание уязвимости;

– ссылки на внешние ресурсы, в которых содержится более детальная информация об уязвимости и (или) рекомендации производителей программных средств по ее устранению.

Существуют модификации базы данных CVE, наиболее популярной из которых является база данных NVD (National Vulnerability Database). Основным отличием базы данных CVE от базы данных NVD является наличие в ней сведений о результатах оценки уязвимостей в соответствии со стандартом CVSS (Common Vulnerability Scoring System). Эти результаты отражены в поле, в котором содержится описание уязвимости. Результат оценки уязвимости в соответствии со стандартом CVSS – это совокупность вектора уязвимости и соответствующей ему оценки по шкале от 1,0 до 10,0, которой, в свою очередь, соответствует критичность уязвимости (чем выше оценка, тем более критичной является уязвимость).

Вектор уязвимости, по своей сути, представляет собой совокупность сведений об условиях и последствиях эксплуатации уязвимости. Выделяют три группы метрик, на основе которых может быть сформирован вектор уязвимости согласно стандарту CVSS:

1) базовые;

2) временные;

3) контекстные.

Ниже представлен пример вектора уязвимости, сформированного на основе базовых метрик согласно версии 3.1 стандарта CVSS (жирным начертанием выделены составляющие вектора, которые являются неизменными):

AV:N / **AC**:H / **PR**:N / **UI**:N / **S**:C / **C**:H / **I**:H / **A**:H.

В табл. 11.2 приведено краткое описание сути каждой из составляющих вектора уязвимости, сформированного на основе базовых метрик согласно версии 3.1 стандарта CVSS, а также значения, которыми они могут характеризоваться.

Таблица 11.2

Характеристики составляющих вектора уязвимости, сформированного на основе базовых метрик согласно версии 3.1 стандарта CVSS

Составляющая	Краткое описание	Значения
1	2	3
AV (Attack Vector)	**Вектор атаки.** Значение, характеризующее эту составляющую, указывает на условие эксплуатации уязвимости (наличие сетевого доступа, или наличие доступа к домену, или наличие локального доступа, или наличие физического доступа к оборудованию системы)	Network (N) Adjacent (A) Local (L) Physical (P)
AC (Attack Complexity)	**Сложность атаки.** Значение, характеризующее эту составляющую, указывает на то, в каком объеме (малом или большом) нарушителю необходимо собрать дополнительные сведения о системе, прежде чем проэксплуатировать уязвимость	Low (L) High (H)
PR (Privileges Required)	**Требуемые привилегии.** Значение, характеризующее эту составляющую, указывает на то, привилегиями какого уровня (никакого, или низкого, или высокого) должен обладать нарушитель для того, чтобы проэксплуатировать уязвимость	None (N) Low (L) High (H)
UI (User Interaction)	**Взаимодействие с пользователем.** Значение, характеризующее эту составляющую, указывает на то, необходимо ли участие легитимного пользователя системы в эксплуатации уязвимости	None (N) Required (R)
S (Scope)	**Область.** Значение, характеризующее эту составляющую, указывает на то, влияет ли эксплуатация уязвимости на состояние информационных ресурсов	Unchanged (U) Changed (C)
C (Confidentiality)	**Свойство конфиденциальности.** Значение, характеризующее эту составляющую, указывает на то, нарушается ли свойство конфиденциальности информационных ресурсов в результате эксплуатации уязвимости	None (N) Low (L) High (H)
I (Integrity)	**Свойство целостности.** Значение, характеризующее эту составляющую, указывает на то, нарушается ли свойство целостности информационных ресурсов в результате эксплуатации уязвимости	None (N) Low (L) High (H)

Окончание табл. 11.2

1	2	3
A (Availability)	**Свойство доступности.** Значение, характеризующее эту составляющую, указывает на то, нарушается ли свойство доступности информационных ресурсов в результате эксплуатации уязвимости	None (N) Low (L) High (H)

Следует отметить, что 1 октября 2023 года была опубликована версия 4.0 стандарта CVSS. Однако в базе данных NVD на момент написания данного учебного пособия (апрель 2024 г.) сведения об уязвимостях не содержали результатов их оценки согласно указанной версии стандарта. Ниже представлен пример вектора уязвимости, сформированного на основе базовых метрик согласно версии 4.0 стандарта CVSS (жирным начертанием выделены составляющие вектора, которые являются неизменными):

AV:N / **AC**:L / **AT**:N / **PR**:L / **UI**:N / **VC**:H / **VI**:H / **VA**:H / **SC**:N / **SI**:N / **SA**:N

В табл. 11.3 представлены краткое описание сути каждой из составляющих вектора уязвимости, сформированного на основе базовых метрик согласно версии 4.0 стандарта CVSS, а также значения, которыми они могут характеризоваться.

Таблица 11.3

Характеристики составляющих вектора уязвимости, сформированного на основе базовых метрик согласно версии 4.0 стандарта CVSS

Составляющая	Краткое описание	Значения
1	2	3
AV (Attack Vector)	**Вектор атаки.** Значение, характеризующее эту составляющую, указывает на условие эксплуатации уязвимости (наличие сетевого доступа, или наличие доступа к домену, или наличие локального доступа, или наличие физического доступа к оборудованию системы)	Network (N) Adjacent (A) Local (L) Physical (P)
AC (Attack Complexity)	**Сложность атаки.** Значение, характеризующее эту составляющую, указывает на то, в каком объеме (малом или большом) нарушителю необходимо собрать дополнительные сведения о системе, прежде чем проэксплуатировать уязвимость	Low (L) High (H)

Продолжение табл. 11.3

1	2	3
AT (Attack Requirements)	**Требования к атаке.** Значение, характеризующее эту составляющую, указывает на то, нужны ли нарушителю особые условия для успешной реализации атаки	None (N) P (present)
PR (Privileges Required)	**Требуемые привилегии.** Значение, характеризующее эту составляющую, указывает на то, привилегиями какого уровня (никакого, или низкого, или высокого) должен обладать нарушитель для того, чтобы проэксплуатировать уязвимость	None (N) Low (L) High (H)
UI (User Interaction)	**Взаимодействие с пользователем.** Значение, характеризующее эту составляющую, указывает на то, необходимо ли участие легитимного пользователя системы в эксплуатации уязвимости; если необходимо, то какое: незначительное (непроизвольные действия) или значительное (сознательные действия)	None (N) Passive (P) Active (A)
VC (Confidentiality)	**Влияние на свойство конфиденциальности информационных ресурсов уязвимой системы.** Значение, характеризующее эту составляющую, указывает на то, нарушается ли свойство конфиденциальности информационных ресурсов в результате эксплуатации уязвимости	None (N) Low (L) High (H)
VI (Integrity)	**Влияние на свойство целостности информационных ресурсов уязвимой системы.** Значение, характеризующее эту составляющую, указывает на то, нарушается ли свойство целостности информационных ресурсов в результате эксплуатации уязвимости	None (N) Low (L) High (H)
VA (Availability)	**Влияние на свойство доступности информационных ресурсов уязвимой системы.** Значение, характеризующее эту составляющую, указывает на то, нарушается ли свойство доступности информационных ресурсов в результате эксплуатации уязвимости	None (N) Low (L) High (H)

Окончание табл. 11.3

1	2	3
SC (Confidentiality)	**Влияние на свойство конфиденциальности информационных ресурсов результирующей системы (т. е. системы, которая сформируется после того, как будет проэксплуатирована уязвимость).** Значение, характеризующее эту составляющую, указывает на то, нарушится ли свойство конфиденциальности информационных ресурсов результирующей системы	None (N) Low (L) High (H)
SI (Integrity)	**Влияние на свойство целостности информационных ресурсов следующей системы.** Значение, характеризующее эту составляющую, указывает на то, нарушится ли свойство целостности информационных ресурсов результирующей системы	None (N) Low (L) High (H)
SA (Availability)	**Влияние на свойство доступности информационных ресурсов следующей системы.** Значение, характеризующее эту составляющую, указывает на то, нарушится ли свойство доступности информационных ресурсов результирующей системы	None (N) Low (L) High (H)

Для обнаружения уязвимостей информационных систем используются программные средства, называемые сканерами уязвимостей. Большинство современных сканеров уязвимостей интегрировано с базой данных CVE, благодаря чему результаты сканирования информационных систем включают в себя сведения из этой базы, т. е. сведения об идентификаторах обнаруженных уязвимостей, краткое описание последних. Примеры сканеров уязвимостей, сертифицированных Оперативно-аналитическим центром при Президенте Республики Беларусь, следующие: XSpider, RedCheck, MaxPatrol.

Контрольные вопросы

1. Что такое информационная система?
2. Что такое информационный ресурс?
3. Какие элементы входят в состав информационной системы?
4. Что такое идентификация?
5. Какие виды идентификаторов выделяют?
6. Что такое аутентификация?
7. Что такое авторизация?
8. Что такое модель управления доступом?
9. Какие выделяют модели управления доступом?
10. Чем обусловлены уязвимости информационных систем?

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Об информации, информатизации и защите информации : Закон Респ. Беларусь от 10 нояб. 2008 г. № 455-З [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=2012&oldDoc=2008-279/2008-279(014-027).pdf&oldDocPage=1. – Дата доступа: 03.02.2024.

2. О государственных секретах : Закон Респ. Беларусь от 19 июля 2010 г. № 170-З [Электронный ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=h11000170&q_id=10679116. – Дата доступа: 03.02.2024.

3. О защите персональных данных : Закон Респ. Беларусь от 7 мая 2021 г. № 99-З [Электронный ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=h12100099&q_id=10679098. – Дата доступа: 03.02.2024.

4. Об утверждении Концепции национальной безопасности Республики Беларусь : Указ Президента Респ. Беларусь от 9 нояб. 2010 г. № 575 [Электронный ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=p31000575&q_id=10679127. – Дата доступа: 03.02.2024.

5. О некоторых мерах по совершенствованию защиты информации : Указ Президента Респ. Беларусь от 16 апр. 2013 г. № 196 [Электронный ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=p31300196. – Дата доступа: 03.02.2024.

6. О мерах по реализации Указа Президента Республики Беларусь от 9 дек. 2019 г. № 449 : приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февр. 2020 г. № 66 [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2020%20-%2066.pdf. – Дата доступа: 03.02.2024.

7. Запечников, С. В. Криптографические методы защиты информации : учебник / С. В. Запечников, О. В. Казарин, А. А. Тарасов. – М. : Юрайт, 2023. – 309 с.

8. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Пресс, 2021. – 262 с.

9. Бутакова, Н. Г. Криптографические методы и средства защиты информации: учеб. пособие / Н. Г. Бутакова, Н. В. Федоров. – СПб. : Интермедия, 2020. – 380 с.

10. Тимофеев, А. М. Криптографическая защита информации: пособие / А. М. Тимофеев. – Минск : БГУИР, 2018. – 44 с.

11. Рябко, Б. Я. Криптография в информационном мире / Б. Я. Рябко, А. Н. Фионов. – М. : Горячая линия-Телеком, 2018. – 300 с.

12. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия / О. Р. Лапонина. – М. : Нац. открытый ун-т «Интуит», 2016. – 244 с.

13. Басалова, Г. В. Основы криптографии / Г. В. Басалова. – М. : Нац. открытый ун-т «Интуит», 2016. – 283 с.

14. Радько, Н. М. Основы криптографической защиты информации : учеб. пособие / Н. М. Радько, А. Н. Мокроусов. – Воронеж : ФГБОУ ВПО ВГУ, 2014. – 109 с.

15. Бабаш, А. В. Криптография / А. В. Бабаш, Г. П. Шанкин ; под ред. А. П. Шерстюка и Э. А. Применко. – М. : СОЛОН-Пресс, 2007. – 512 с.

16. Пулко, Т. А. Введение в информационную безопасность : учеб. пособие / Т. А. Пулко. – Минск : БГУИР, 2016. – 164 с.

17. Новиков, В. К. Информационная безопасность и защита информации: организационно-правовые основы / В. К. Новиков, И. Б. Галушкин, С. В. Аксенов. – М. : Горячая линия-Телеком, 2016. – 312 с.

18. Петраков, А. В. Основы практической защиты информации : учеб. пособие / А. В. Петраков. – 4-е изд. – М. : СОЛОН-Пресс, 2005. – 384 с.

19. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 3-е изд. – М. : Академия, 2008. – 336 с.

Св. план 2025, поз. 27

Учебное издание

Борботько Тимофей Валентинович
Бойправ Ольга Владимировна
Тимофеев Александр Михайлович

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УЧЕБНОЕ ПОСОБИЕ

Редактор *Ю. В. Граховская*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *Е. Г. Бабичева*

Подписано в печать 30.06.2025. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 7,56. Уч.-изд. л. 8,0. Тираж 200 экз. Заказ 5.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск