

## Содержание:

# ВВЕДЕНИЕ

Новые информационные технологии бурными темпами внедряются во все сферы деятельности жизни людей. Появление локальных и глобальных сетей передачи данных предоставило пользователям компьютеров новые возможности оперативного обмена информацией. Если до недавнего времени подобные сети создавались только в специфических и узконаправленных целях (университетские сети, сети военных ведомств, спецслужб и так далее), то развитие Интернета и аналогичных систем привело к использованию глобальных сетей передачи данных в повседневной жизни практически каждого человека. Информация, как ресурс, несет в себе значительную ценность, поэтому при нынешней информатизации общества очень важно сохранить целостность и неприкосновенность передаваемой информации.

Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Проблемы, возникающие с безопасностью передачи информации при работе в компьютерных сетях, можно разделить на три основных типа:

- перехват информации – целостность информации сохраняется, но её конфиденциальность нарушена;
- модификация информации – исходное сообщение изменяется либо полностью подменяется другим и отсылается адресату;
- подмена авторства информации. Данная проблема может иметь серьёзные последствия. Например, кто-то может послать письмо от вашего имени (этот вид обмана принято называть спуфингом) или Web – сервер может притворяться электронным магазином, принимать заказы, номера кредитных карт, но не высылать никаких товаров.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это обратная сторона использования информационных технологий.

Выборочная и бессистемная реализация мероприятий, направленных на повышение уровня IT-безопасности, не сможет обеспечить необходимого уровня защиты. Чтобы сформировать понимание приоритетности мероприятий по повышению уровня безопасности, необходимо разработать механизм управления рисками IT-безопасности, что позволит направить все усилия на защиту от наиболее опасных угроз и минимизацию затрат.

Актуальность и важность проблемы обеспечения информационной безопасности обусловлена следующими факторами:

- увеличение рисков информационной безопасности в связи с появлением новых и изощренных угроз для информационной безопасности;
- современные темпы и уровни развития средств информационной безопасности значительно отстают от темпов и уровней развития информационных технологий;
- быстрые темпы роста парка персональных компьютеров, применяемых в разнообразных сферах человеческой деятельности из-за увеличения обрабатываемой информации;
- резкое расширение сферы пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;
- доступность корпоративной информации через мобильные устройства (ноутбук, КПК, смартфон).
- доступность средств персональных ЭВМ, привела к распространению компьютерной грамотности в широких слоях населения.
- значительное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации.
- стремительное развитие информационных технологий, открыло новые возможности эффективной работы предприятия, однако привело и к появлению новых угроз.

Анализа угроз информационной безопасности позволяет определить, какие мероприятия эффективны для их минимизации и предотвращения, а какие нет.

Целью данной курсовой работы является изучение теоретических основ информационной безопасности, а также рассмотрение видов и состава угроз информационной безопасности.

Для достижения поставленной цели требуется решить следующие основные задачи:

- ознакомиться теоретическими основами информационной безопасности,
- изучить особенности различных видов угроз информационной безопасности,
- проанализировать состав угроз информационной безопасности,
- сделать выводы по работе.

В работе использована учебно-методическая литература и Интернет-ресурсы.

## **ГЛАВА 1. КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Анализ состояния дел в сфере защиты информации показывает, что уже сложилась вполне сформировавшаяся концепция и структура, основу которой составляют:

- весьма развитый арсенал технических средств защиты информации, производимых на промышленной основе;
- значительное число фирм, специализирующихся на решении вопросов защиты информации;
- достаточно четко очерченная система взглядов на эту проблему;
- наличие значительного практического опыта и другое.

Тем не менее, как свидетельствует отечественная и зарубежная печать, злоумышленные действия над информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту.

Основные понятия теории информационной безопасности

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий. В свою очередь защита

информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности[1].

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Кроме того, защита информации понимается как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

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

Способ защиты информации - порядок и правила применения определенных принципов и средств защиты информации.

Защита информации от утечки - защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации (иностранными) разведками и другими заинтересованными субъектами.

Защита информации от разглашения - защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа - защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Система защиты информации - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Безопасность информации (данных) - состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Политика безопасности (информации в организации) - совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности [\[2\]](#).

Опасности - возможные или реальные явления, события и процессы, способные нанести ущерб или уничтожить индивида, социальную группу, народ, общество, государство и человечество в целом, нанести ущерб благополучию, разрушить материальные, духовные или природные ценности, вызвать деградацию, закрыть путь к развитию науки в целом. Опасности родственно понятие «угроза»; угрозы исходят от различного рода источников опасности.

В зависимости от типа угрозы, а также в содержательном плане для международной и национальной безопасности, выделяются следующие сферы (области) ее проявления и обеспечения:

- экологическая безопасность;
- экономическая безопасность;
- военная безопасность;
- ресурсная безопасность;
- информационная безопасность;
- социальная безопасность;
- научно-техническая безопасность;
- энергетическая безопасность;
- ядерная безопасность;

- политическая безопасность;
- инновационная безопасность;
- правовая безопасность;
- культурная безопасность;
- техническая безопасность и др.

Многообразие объектов защиты, множество опасностей и угроз, а также их источников в настоящее время выдвигает на первый план необходимость разработки общетеоретических основ обеспечения безопасности. Постановка любой новой проблемы требует выделения базовых вопросов. Их методологическое осмысление позволяет понять проблему в целом и выйти на ее практическое, прикладное решение.

Основой современной концепции безопасности в условиях глобализации является единство отношений основных социальных субъектов - личность, организация, общество, государство и мировое сообщество в целом.

Методологию безопасности можно сформулировать как учение об основах, принципах, структуре, логической организации системы безопасности, видах и методах деятельности по ее обеспечению.

Особое значение информационная безопасность приобретает в условиях коммерческой деятельности. Информация об изменении политической, социальной, экономической и экологической ситуации, изменения рынков организации, научно-техническая и технологическая информация, конкретные ноу-хау, касающиеся каких-либо аспектов бизнеса, новое в методах организации и управления бизнесом позволяет адекватно реагировать на любые изменения внешней среды бизнеса, эффективно планировать и осуществлять свою хозяйственную деятельность.

Факторы бизнеса, используемые владельцами организации для выполнения целей бизнеса: ресурс капитала, ресурс персонала, ресурс информации и технологии являются корпоративными ресурсами. Эта информация, касающаяся всех сторон деятельности предприятия и организации, в настоящее время наиболее ценный и дорогостоящий ресурс, требующий принятия определенных мер по защите.

Таким образом, в настоящее время сложилась система взглядов на обеспечение информационной безопасности. В то же время злоумышленные действия над информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту, что определяет актуальность оценки угроз информационной безопасности[3].

## Составляющие информационной безопасности

Информационная безопасность (ИБ) – многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только систематический, комплексный подход. Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Иногда в число основных составляющих ИБ включают защиту от несанкционированного копирования информации, но, на наш взгляд, это слишком специфический аспект с сомнительными шансами на успех, поэтому не станем его выделять. Поясним понятия доступности, целостности и конфиденциальности. Доступность – это возможность за приемлемое время получить требуемую информационную услугу. Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. Наконец, конфиденциальность – это защита от несанкционированного доступа к информации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, выделяем ее как важнейший элемент информационной безопасности. Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.). Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)).

Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений. Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит "руководством к действию". Рецепт лекарства, предписанные медицинские

процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Неприятно и искажение официальной информации, будь то текст закона или страница Web-сервера какой-либо правительственной организации.

К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы. Если вернуться к анализу интересов различных категорий субъектов информационных отношений, то почти для всех, кто реально использует ИС, на первом месте стоит доступность[\[4\]](#).

Понимая информационную безопасность как «состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций», правомерно определить угрозы безопасности информации, источники этих угроз, способы их реализации и цели, а также иные условия и действия, нарушающие безопасность. При этом, естественно, следует рассматривать и меры защиты информации от неправомерных действий, приводящих к нанесению ущерба.

Практика показала, что для анализа такого значительного набора источников, объектов и действий целесообразно использовать методы моделирования, при которых формируется как бы «заместитель» реальных ситуаций. При этом следует учитывать, что модель не копирует оригинал, она проще. Модель должна быть достаточно общей, чтобы описывать реальные действия с учетом их сложности.

Можно предложить компоненты модели информационной безопасности на первом уровне декомпозиции. По нашему мнению, такими компонентами концептуальной модели безопасности информации могут быть следующие:

- объекты угроз;
- угрозы;
- источники угроз;
- цели угроз со стороны злоумышленников;

- источники информации;
- способы неправомерного овладения конфиденциальной информацией (способы доступа);
- направления защиты информации;
- способы защиты информации;
- средства защиты информации.

Объектом угроз информационной безопасности выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, материальных и финансовых ценностей, информационных ресурсов).

Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности.

Источниками угроз выступают конкуренты, преступники, коррупционеры, административно-управленческие органы.

Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба.

Неправомерное овладение конфиденциальной информацией возможно за счет ее разглашения источниками сведений, за счет утечки информации через технические средства и за счет несанкционированного доступа к охраняемым сведениям.

Источниками конфиденциальной информации являются люди, документы, публикации, технические носители информации, технические средства обеспечения производственной и трудовой деятельности, продукция и отходы производства.

Основными направлениями защиты информации являются правовая, организационная и инженерно-техническая защиты информации как выразители комплексного подхода к обеспечению информационной безопасности.

Средствами защиты информации являются физические средства, аппаратные средства, программные средства и криптографические методы. Последние могут быть реализованы как аппаратно, программно, так и смешанно-программно-аппаратными средствами.

Особенности защищаемой информации

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

В соответствии со статьей 128. Гражданского кодекса РФ к объектам гражданских прав относятся вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права; работы и услуги; информация; результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность), нематериальные блага[5].

Обладатель информации вправе:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации обязан:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Информация в зависимости от категории доступа к ней подразделяется на:

- общедоступную информацию;
- информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).
- Информация в зависимости от порядка ее предоставления или распространения подразделяется на:
  - информацию, свободно распространяемую;
  - информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
  - информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
  - информацию, распространение которой в РФ ограничивается или запрещается.

Информация - это ресурс. Потеря конфиденциальной информации приносит моральный или материальный ущерб. Условия, способствующие неправомерному овладению конфиденциальной информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам.

Многообразие условий, способствующих неправомерному овладению конфиденциальной информацией, вызывает необходимость подробного и глубокого изучения видов и источников угроз информационной безопасности, так как бороться с нарушением информационной безопасности можно лишь зная, откуда эта опасность берет свое начало[6].

## **Глава 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Носителями угроз безопасности информации являются источники угроз. Под угрозой информационной безопасности принято понимать потенциально возможные действия, явления или процессы, способные оказать нежелательное воздействие на систему или на хранящуюся в ней информацию. В качестве источников угроз могут выступать как субъекты (личность) так и объективные проявления. Причем, источники угроз могут находиться как внутри защищаемой организации - внутренние источники, так и вне ее - внешние источники.

Под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Фактор, воздействующий на защищаемую информацию - явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

Источник угрозы безопасности информации - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Уязвимость информационной системы (брешь) - свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации[7].

Классификация угроз информационной безопасности

По отношению к информации и информационным ресурсам можно выделить угрозы целостности, конфиденциальности, достоверности и доступности информации, проявляющиеся в различных формах нарушений (рис. 1.).

## **Угрозы информационной**

### **безопасности**

#### **Проявляются в нарушениях**

ЦЕЛОСТНОСТИ

КОНФИДЕНЦИАЛЬНОСТИ

ДОСТУПНОСТИ

1. Разглашение
2. Утечка
3. НДС
4. Искажения
5. Ошибки
6. Потери
7. Фальсификации
8. Нарушение связи
9. Воспреещение получения

**Рисунок 1. Влияние угроз информации на критерии информационной безопасности**

Как правило, вышеперечисленные угрозы информационным ресурсам реализуются следующими способами:

- Через имеющиеся агентурные источники в органах государственного управления и коммерческих структурах, имеющих возможность получения конфиденциальной информации (суды, налоговые органы, коммерческие банки и т. д.).
- Путем подкупа лиц, непосредственно работающих в организации или структурах, напрямую связанных с ее деятельностью.
- Путем перехвата информации, циркулирующей в средствах и системах связи и вычислительной технике с помощью технических средств разведки и съема информации.
- Путем прослушивания конфиденциальных переговоров и другими способами несанкционированного доступа к источникам конфиденциальной информации.

Информационная безопасность оказывает влияние на защищенность интересов в различных сферах жизнедеятельности общества и государства. В каждой из них имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности.

Например, с позиции обеспечения безопасности информации в компьютерных системах (КС) все множество потенциальных угроз безопасности информации в КС может быть разделено на два класса.

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют случайными или непреднамеренными.

Реализация угроз этого класса приводит к наибольшим потерям информации (по статистическим данным - до 80% от ущерба, наносимого информационным ресурсам КС любыми угрозами). При этом могут происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию.

Стихийные бедствия и аварии чреватые наиболее разрушительными последствиями для информации, так как носители подвергаются физическому разрушению, информация утрачивается или доступ к ней становится невозможен.

Сбои и отказы сложных систем неизбежны. В результате сбоев и отказов нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы, нарушается алгоритм работы устройств. Нарушения алгоритмов работы отдельных узлов и устройств могут также привести к нарушению конфиденциальности информации. Например, сбои и отказы средств выдачи информации могут привести к несанкционированному доступу к информации путем несанкционированной ее передачи в канал связи, на печатающее устройство и т. п.

Ошибки при разработке КС, алгоритмические и программные ошибки приводят к последствиям, аналогичным последствиям (сбоев и отказов технических средств). Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы КС. Особую опасность представляют ошибки в операционных системах (ОС) и в программных средствах защиты информации.

Согласно данным Национального института стандартов и технологий США (NIST) 65% случаев нарушения безопасности информации происходит в результате ошибок пользователей и обслуживающего персонала. Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводят к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты[8].

Другой класс угроз безопасности информации в компьютерных системах составляют преднамеренно создаваемые угрозы. Угрозы этого класса в соответствии с их физической сущностью и механизмами реализации могут быть распределены по пяти группам:

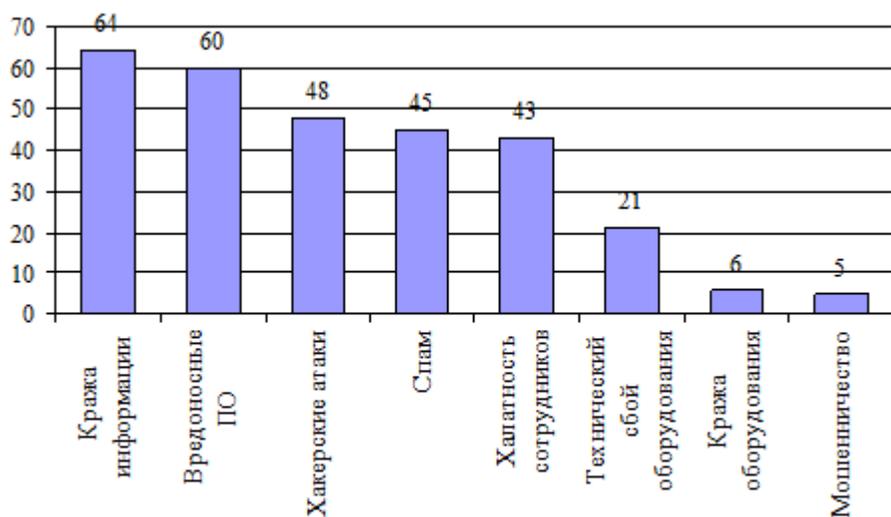
- традиционный или универсальный шпионаж и диверсии;
- несанкционированный доступ к информации;
- электромагнитные излучения и наводки;
- модификация структур;
- вредоносные программы.

Источники угроз информационной безопасности

В качестве источников нежелательного воздействия на информационные ресурсы по-прежнему актуальны методы и средства шпионажа и диверсий, которые использовались и используются для добывания или уничтожения информации. Эти методы также действенны и эффективны в условиях применения компьютерных систем. Чаще всего они используются для получения сведений о системе защиты с

целью проникновения в систему, а также для хищения и уничтожения информационных ресурсов.

Согласно статистике применительно к угрозам информационной безопасности, можно привести следующие данные (по результатам исследований, проведённых в России компанией InfoWatch, 2015 г.):



## Рисунок 2. Источники угроз информационной безопасности

В настоящее время основными источниками угроз для информации на компьютере пользователя является интернет и электронная почта. Огромное количество вредоносных программ, в число которых входят вирусы, троянские программы, черви, могут "пробраться" на компьютер, пока пользователь читает статью в интернете, занимается поиском информации, открывая множество веб-сайтов, скачивает и устанавливает программное обеспечение на компьютер, читает почтовое сообщение. Вредоносные программы распространяются с молниеносной скоростью и за доли секунды могут нанести такой вред, восстановление после которого может дорого обойтись. Речь здесь идет не только о повреждении данных, но и о несанкционированном доступе к системе, нарушении ее целостности, краже информации.

Не стоит забывать и о еще одном важном источнике "неприятностей" - спаме. Нежелательная почтовая корреспонденция может нанести гораздо больший вред, чем некоторые вредоносные программы. Не являясь источником прямой угрозы, спам приводит к потерям рабочего времени и наносит значительные финансовые потери, которые увеличиваются в сотни, тысячи раз, если это касается корпоративной компьютерной сети.

Каждый пользователь, широко использующий современные информационные ресурсы, должен знать, что ему угрожает и какие последствия может за собой повлечь то или иное вредоносное воздействие.

Угрозы в коммерческой деятельности также имеют свои особенности. По отношению к отдельной организации существуют следующие основные виды внешних угроз:

- Недобросовестные конкуренты.
- Криминальные группы и формирования.
- Противозаконные действия отдельных лиц и организаций административного аппарата, в том числе и налоговых служб.
- Нарушение установленного регламента сбора, обработки и передачи информации.

Основные виды внутренних угроз:

- Преднамеренные преступные действия собственного персонала организации.
- Непреднамеренные действия и ошибки сотрудников.
- Отказ оборудования и технических средств.
- Сбои программного обеспечения средств обработки информации.

Внутренние и внешние угрозы тесно взаимодействуют. Например, общая тенденция криминализации хозяйственной деятельности ведет к снижению морально-этических норм сотрудников всех рангов, часто толкает их на действия, наносящие ущерб предприятию.

Соотношение внутренних и внешних угроз в соответствии с характеризуется следующими показателями:

81,7% угроз совершается либо самими сотрудниками организаций, либо при их прямом или опосредованном участии (внутренние угрозы);

17,3% угроз — внешние угрозы или преступные действия;

1,0% угроз — угрозы со стороны случайных лиц[9].

Объектами различных угроз в коммерческой деятельности являются:

- Человеческие ресурсы (персонал, сотрудники, компаньоны и др.), включая трудовые и кадровые ресурсы.

- Материальные ресурсы.
- Финансовые ресурсы.
- Временные ресурсы.

Информационные ресурсы, включая интеллектуальные ресурсы (патенты, незавершенные проектно-конструкторские разработки, ноу-хау, программные продукты, массивы бухгалтерской и статистической информации и пр.).

Наиболее опасным источником угроз предприятиям выступают собственные сотрудники. Мотивами внутренних угроз в этом случае являются безответственность, некомпетентность (низкая квалификация), личные побуждения (самоутверждение, корыстные интересы).

В условиях сохраняющейся высокой степени монополизации российской экономики опасность предпринимательству представляет недобросовестная конкуренция, представляющая собой:

- Все действия, ведущие к тому, что потребитель может принять предприятие, товары, промышленную или коммерческую деятельность данной организации за предприятие, товары, промышленную или коммерческую деятельность конкурента.
- Ложные заявления в ходе коммерческой деятельности, дискредитирующие предприятие, товары, промышленную или коммерческую деятельность конкурента.
- Использование в ходе коммерческой деятельности указаний или обозначений, которые вводят потребителя в заблуждение относительно природы, способа изготовления, характеристик, пригодности для определенных целей или количества товаров.

Реализация угроз в данном случае снижает эффективность и надежность функционирования организаций, а в отдельных случаях, приводят к прекращению их деятельности из-за опасности экономического, социального, правового, организационного, информационного, экологического, технического и криминального характера. Объектами угроз могут быть элементы вещественного, личного («человеческого»), финансового, информационного и иного капитала, составляющего экономическую основу деятельности предпринимательства.

Вредоносные программы

Вредоносные программы (Malware — сокращение от "malicious software") - любое программное обеспечение, специально созданное для того, чтобы причинять ущерб компьютеру, серверу или компьютерной сети, хранящимся на них данным, независимо от того, является ли оно вирусом, трояном, сетевым червем и т. д.[\[10\]](#).

**Таблица 1. TOP 10 стран по числу атакованных пользователей (Источник Kaspersky Security Bulletin 2014. Основная статистика за 2014 год)**

<b>Страна</b>	<b>% атакованных пользователей*</b>
1 Россия	45,7%
2 Индия	6,8%
3 Казахстан	4,1%
4 Германия	4,0%
5 Украина	3,0%
6 Вьетнам	2,7%
7 Иран	2,3%
8 Великобритания	2,2%
9 Малайзия	1,8%
10 Бразилия	1,6%

\* Процент пользователей, атакованных в стране, от всех атакованных пользователей

Одних только типов вредоносных программ известно великое множество. Но каждый тип состоит из огромного количества образцов, также отличающихся друг от друга. Для борьбы со всеми ними нужно уметь однозначно классифицировать любую вредоносную программу и легко отличить ее от других вредоносных программ[11]. В целом вредоносные программы можно разделить на следующие классы:

**Вирусы (Viruses):** программы, которые заражают другие программы - добавляют в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом - заражение. Скорость распространения вирусов несколько ниже, чем у червей.

**Черви (Worms):** данная категория вредоносных программ для распространения использует сетевые ресурсы. Название этого класса было дано исходя из способности червей "переползать" с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Также благодаря этому черви обладают исключительно высокой скоростью распространения.

Черви проникают на компьютер, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

**Троянские программы (Trojans):** программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к "зависанию", воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом "полезного" программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

**Программы-шпионы (Spyware):** программное обеспечение, позволяющее собирать сведения об отдельно взятом пользователе или организации без их ведома. О

наличии программ-шпионов на своем компьютере вы можете и не догадываться. Как правило, целью программ-шпионов является:

- отслеживание действий пользователя на компьютере;
- сбор информации о содержании жесткого диска; в этом случае чаще всего речь идет о сканировании некоторых каталогов и системного реестра с целью составления списка программного обеспечения, установленного на компьютере;
- сбор информации о качестве связи, способе подключения, скорости модема и т.д.

Однако данные программы не ограничиваются только сбором информации, они представляют реальную угрозу безопасности. Как минимум две из известных программ - Gator и eZula - позволяют злоумышленнику не просто собирать информацию, но и контролировать чужой компьютер. Другим примером программ-шпионов являются программы, встраивающиеся в установленный на компьютере браузер и перенаправляющие трафик.

Одной из разновидностей программ-шпионов являются фишинг-рассылки. Фишинг (Phishing) - почтовая рассылка, целью которой является получение от пользователя конфиденциальной информации как правило финансового характера. Такие письма составляются таким образом, чтобы максимально походить на информационные письма от банковских структур, компаний известных брендов. Письма содержат ссылку на заведомо ложный сайт, где пользователю предлагается ввести, например, номер своей кредитной карты и другую конфиденциальную информацию.

Программы-рекламы (Adware): программный код, без ведома пользователя включенный в программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе.

Потенциально опасные приложения (Riskware): программное обеспечение, не являющееся вирусом, но содержащее в себе потенциальную угрозу. При некоторых условиях наличие таких программ на компьютере подвергает ваши данные риску. К таким программам относятся утилиты удаленного администрирования, программы автоматического дозвона на платные ресурсы интернета с

использованием Dial Up-соединения и другие.

Программы-шутки (Jokes): программное обеспечение, не причиняющее компьютеру какого-либо прямого вреда, но выводящее сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях. Такие программы часто предупреждают пользователя о несуществующей опасности, например, выводят сообщения о форматировании диска (хотя никакого форматирования на самом деле не происходит), обнаруживают вирусы в незараженных файлах и т.д.

Программы-маскировщики (Rootkit): это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Rootkit'ы также могут модифицировать операционную систему на компьютере и заменять основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Прочие опасные программы: разнообразные программы, которые разработаны для создания других вредоносных программ, организации DoS-атак на удаленные сервера, взлома других компьютеров и т. п. К таким программам относятся хакерские утилиты (Hack Tools), конструкторы вирусов и т.д.

Спам (Spam): анонимная, массовая почтовая корреспонденция нежелательного характера. Так, спамом являются рассылки политического и агитационного характера, письма, призывающие помочь кому-нибудь. Отдельную категорию спама составляют письма с предложениями обналичить большую сумму денег или вовлекающие в финансовые пирамиды, а также письма, направленные на кражу паролей и номеров кредитных карт, письма с просьбой переслать знакомым (например, письма счастья) и т. п. Спам существенно повышает нагрузку на почтовые сервера и повышает риск потери информации, важной для пользователя.

Вирус – это наиболее распространенный вид вредоносных программ.

Компьютерный вирус - это специально написанная, небольшая по размерам, программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала, как правило, управление получает вирус. Вирус находит и "заражает" другие программы или выполняет какие-нибудь вредные функции: портит файлы или таблицу размещения файлов на диске, "засоряет" оперативную память, изменяет адресацию обращений

к внешним устройствам и т.д. Более того, зараженные программы могут быть перенесены на другой компьютер с помощью дискет или локальной сети.

В настоящее время известно более двадцати тысяч вирусов. Условно они подразделяются на классы по следующим признакам.

По среде обитания:

- сетевые, распространяющиеся по компьютерной сети;
- файловые, внедряющиеся в выполняемый файл;
- загрузочные, внедряющиеся в загрузочный сектор жесткого диска или дискеты.

По способу заражения:

- резидентные, загружаемые в память ПК;
- нерезидентные, не заражающие память ПК и остающиеся активными ограниченное время

По возможностям:

- безвредные, не влияющие на работу ПК;
- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими звуковыми и прочими эффектами;
- опасные, которые могут привести к серьезным сбоям в работе ПК;
- очень опасные, которые могут привести к потере программ, уничтожению данных, стереть информацию в системных областях памяти и даже преждевременному выходу из строя периферийных устройств.

Данная классификация объединяет, естественно, далеко не, все возможные вирусы; в каждой категории встречаются варианты, не названные в силу их экзотичности, например, CMOS-вирусы или вирусоподобные структуры, "обитающие" в среде Microsoft Word. Кроме того, встречается ряд программ, не обладающих всеми свойствами вирусов, но могущих представлять серьезную опасность ("троянские кони" и т.п.).

В конечном итоге все противоправные действия приводят к нарушению конфиденциальности, достоверности, целостности и доступности информации.

Таким образом, перечень угроз и источников их возникновения достаточно разнообразен и предложенная классификация не является исчерпывающей.

Противодействие проявлениям угроз осуществляется по различным направлениям, с использованием полного арсенала методов и средств защиты.

## **ЗАКЛЮЧЕНИЕ**

Информация - это ресурс. Потеря конфиденциальной информации приносит моральный или материальный ущерб. Условия, способствующие неправомерному овладению конфиденциальной информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам. В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системной защитой информации. Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др. Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях.

Многообразие условий, способствующих неправомерному овладению конфиденциальной информацией, вызывает необходимость использования не менее многообразных способов, сил и средств для обеспечения информационной безопасности.

Носителями угроз безопасности информации являются источники угроз. Под угрозой информационной безопасности принято понимать потенциально возможные действия, явления или процессы, способные оказать нежелательное воздействие на систему или на хранящуюся в ней информацию.

Перечень угроз и источников возникновения информационной опасности достаточно разнообразен. Одних только типов вредоносных программ известно великое множество. Но каждый тип состоит из огромного количества образцов, также отличающихся друг от друга. Для борьбы со всеми ними нужно уметь однозначно классифицировать любую вредоносную программу и легко отличить ее от других вредоносных программ. В целом вредоносные программы можно разделить на следующие классы:

- Вирусы (Viruses)
- Черви (Worms)
- Троянские программы (Trojans),

- Программы-шпионы (Spyware)
- Фишинг (Phishing),
- Программы-рекламы (Adware),
- Потенциально опасные приложения (Riskware),
- Программы-шутки (Jokes),
- Программы-маскировщики (Rootkit),
- Спам (Spam),

и прочие опасные программы.

В конечном итоге все противоправные действия приводят к нарушению конфиденциальности, достоверности, целостности и доступности информации.

Опыт показывает, что для достижения эффективных решений по защите информации необходимо сочетание правовых, организационных и технических мероприятий. То есть обеспечение защиты информации и в целом информационной безопасности современных информационных систем требует комплексного подхода. Оно невозможно без применения широкого спектра защитных средств, объединенных в продуманную архитектуру

В этих условиях позиция по отношению к защите информации должна быть особенно динамичной. Теоретические воззрения, стандарты, сложившиеся порядки необходимо постоянно сверять с требованиями практики. От возможных атак на информацию не защититься без систематической и целенаправленной работы в данном направлении. Реальное состояние безопасности требует каждодневного внимания всех заинтересованных сторон.

## **СПИСОК ЛИТЕРАТУРЫ**

1. Барабанов А. С. Инструментальные средства проведения испытаний систем по требованиям безопасности информации. М.: Защита информации. INSIDE, 2011. — с. 24-36.
2. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010. — с. 124-129.
3. Гладких А.А., В.Е. Дементьев / Базовые принципы информационной безопасности вычислительных сетей: учебное пособие для студентов; - Ульяновск: изд-во УлГТУ, 2011. — с. 18-31.









































































Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

1. Ерохин В. В., Погонышева Д. А., Степченко И. Г.. Безопасность информационных систем. Учебное пособие. — М.: Флинта, Наука, 2015. — с. 85-89.

Текст данного реферата совершенно новый, также планируется дальнейшее развитие Текст данного реферата совершенно новый, также планируется дальнейшее развитие Текст данного реферата совершенно новый, также планируется дальнейшее развитие Текст данного реферата совершенно новый, также планируется дальнейшее развитие Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие





Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

1. Мельников Д. А. Организация и обеспечение безопасности информационно-технологических сетей и систем. — М.: КДУ, 2015. — с. 147-149.

Текст данного реферата совершенно новый, также планируется дальнейшее развитие Текст данного реферата совершенно новый, также планируется дальнейшее развитие Текст данного реферата совершенно новый, также планируется дальнейшее развитие Текст данного реферата совершенно новый, также планируется дальнейшее развитие Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие













Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

1. Оголюк А.А., А.В. Щеглов / Технология и программный комплекс защиты рабочих станций. – М.: изд-во Финансы и статистика, 2011. — с. 252-265.

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие































Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

1. Петренко С.А., Симонов С.В. /Управление информационными рисками. Экономически оправданная безопасность – М.: Радио и связь, 2012. — с. 187-193.

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

































Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2014. — с. 63-71.

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие





Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

1. Симонов С.В. Технологии аудита информационной безопасности // Конфидент. Защита информации. – №2. М.: Издательство СИП РИА – 2013. — с. 12-30.

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие







































Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

1. Трубачев А.П., Долинин М.Ю., Кобзарь М.Т., Сидак А.А., Сороковиков В.И. Оценка безопасности информационных технологий / Под общ. ред. В.А. Галатенко. – М.: Издательство СИП РИА, 2011. — с. 85-101.

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

























Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

1. Храмов В.В. Информационная безопасность и защита информации  
Методическое пособие. — Ростов на Дону.: РГУПС, 2011. — с. 74-100.

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие













дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

1. Шахалов И.Ю. Лицензирование деятельности по технической защите конфиденциальной информации. - М.: Вопросы кибербезопасности, 2013. — с. 121-130.
2. Щеглов А.Ю. / Защита информации от несанкционированного доступа. - М.: изд-во Гелиос АРВ, 2014. — с. 203-210.

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие





Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие  
Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

Текст данного реферата совершенно новый, также планируется дальнейшее развитие

1. Официальный сайт первого в России независимого информационно-аналитический центра [Электронный ресурс]. – Режим доступа: <https://www.anti-malware.ru/malware>
2. Securelist – все об интернет-безопасности [Электронный ресурс]. – Режим доступа: <https://securelist.ru/analysis/ksb/24580/kaspersky-security-bulletin-2014-osnovnaya-statistika-za-2014-god/>

1. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010. — с. 124-129. [↑](#)

2. Оголюк А.А., А.В. Щеглов / Технология и программный комплекс защиты рабочих станций. – М.: изд-во Финансы и статистика, 2011. — с. 252-265. [↑](#)
3. Трубачев А.П., Долинин М.Ю., Кобзарь М.Т., Сидак А.А., Сороковиков В.И. Оценка безопасности информационных технологий / Под общ. ред. В.А. Галатенко. – М.: Издательство СИП РИА, 2011. — с. 85-101. [↑](#)
4. Щеглов А.Ю. / Защита информации от несанкционированного доступа. – М.: изд-во Гелиос АРВ, 2014. — с. 203-210. [↑](#)
5. Мельников Д. А. Организация и обеспечение безопасности информационно-технологических сетей и систем. — М.: КДУ, 2015. — с. 147-149. [↑](#)
6. Гладких А.А., В.Е. Дементьев / Базовые принципы информационной безопасности вычислительных сетей: учебное пособие для студентов; – Ульяновск: изд-во УлГТУ, 2011. — с. 18-31. [↑](#)
7. Ерохин В. В., Погонышева Д. А., Степченко И. Г. Безопасность информационных систем. Учебное пособие. — М.: Флинта, Наука, 2015. — с. 85-89. [↑](#)
8. Шахалов И.Ю. Лицензирование деятельности по технической защите конфиденциальной информации. - М.: Вопросы кибербезопасности, 2013. — с. 121-130. [↑](#)
9. Официальный сайт первого в России независимого информационно-аналитического центра [Электронный ресурс]. – Режим доступа: <https://www.anti-malware.ru/malware> [↑](#)
10. Официальный сайт первого в России независимого информационно-аналитического центра [Электронный ресурс]. – Режим доступа: <https://www.anti-malware.ru/malware> [↑](#)
11. Securelist – все об интернет-безопасности [Электронный ресурс]. – Режим доступа: <https://securelist.ru/analysis/ksb/24580/kaspersky-security-bulletin-2014->

osnovnaya-statistika-za-2014-god/ [↑](#)