|  |
| --- |
| РГПУ им. А.И. Герцена |
| Лабораторная работа №4 |
|  |

|  |
| --- |
| Роман Косоруков Сергеевич  12.12.2017 |

Оглавление

[Глава 1 2](#_Toc500838388)

[Глава 2 3](#_Toc500838389)

[Глава 3 4](#_Toc500838390)

# Глава 1

В системе обеспечения безопасности предпринимательской деятельности все большее значение приобретает обеспечение компьютерной безопасности. Это связано с возрастающим объемом поступающей информации, совершенствованием средств ее хранения, передачи и обработки. Перевод 6значительной части информации в электронную форму, использование локальных и глобальных сетей создают качественно новые угрозы конфиденциальной информации.

[Компьютерные преступления](https://studfiles.net/preview/5771038/) в этом аспекте можно охарактеризовать как противоправные посягательства на экономическую безопасность предпринимательства, в которых объектом, либо орудием преступления является компьютер.

Источник данного вида угроз может быть внутренним (собственные работники), внешним (например, конкуренты), смешанным (заказчики – внешние, а исполнитель – работник фирмы). Как показывает практика, подавляющее большинство таких преступлений совершается самими работниками фирм.

Что же является непосредственным объектом компьютерных преступлений? Им может являться как информация (данные), так и сами компьютерные программы.

Преступник получает доступ к охраняемой информации без разрешения ее собственника или владельца, либо с нарушением установленного порядка доступа. Способы такого неправомерного доступа к компьютерной информации могут быть различными – кража носителя информации, нарушение средств защиты информации, использование чужого имени, изменение кода или адреса технического устройства, представление фиктивных документов на право доступа к информации, установка аппаратуры записи, подключаемой к каналам передачи данных. Причем доступ может быть осуществлен в помещениях фирмы, где хранятся носители, из компьютера на рабочем месте, из локальной сети, из глобальной сети.



Все угрозы на объекты информационной безопасности по способу воздействия могут быть объединены в пять групп: собственно, информационные, физические, организационно-правовые, программно-математические, радиоэлектронные.

Последствия совершенных противоправных действий могут быть различными:

копирование информации (оригинал при этом сохраняется);

изменение содержания информации по сравнению с той, которая была ранее;

блокирование информации – невозможность ее использования при сохранении информации;

уничтожение информации без возможности ее восстановления;

нарушение работы ЭВМ, системы ЭВМ или их сети.

Большую опасность представляют также компьютерные вирусы, то есть программы, которые могут приводить к несанкционированному воздействию на информацию, либо [ЭВМ](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%BE-%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%B0) (системы ЭВМ и их сети), с теми же последствиями

Правовое обеспечение безопасности предпринимательской деятельности от компьютерных преступлений основывается на том, что по российскому законодательству защите подлежит любая документированная информация, неправомерное обращение к которой может нанести ущерб ее собственнику, владельцу, пользователю. Защита осуществляется в целях утечки, хищения, утраты, искажения, подделки информации, а также предотвращения несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращения других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечения правового режима документированной информации как объекта собственности.

Кроме того, за перечисленные выше противоправные действия предусмотрена уголовная ответственность. И это представляется не случайным, поскольку угрозы компьютерным системам могут привести не только к значительным финансовым потерям, но и к необратимым последствиям - ликвидации самого субъекта предпринимательства.

# Глава 2

[Угрозы компьютерным системам](http://3ys.ru/metody-strukturnogo-proektirovaniya-avtomatizirovannykh-sistem-obrabotki-informatsii-i-upravleniya-asoiu/ugrozy-bezopasnosti-v-kompyuternykh-sistemakh.html) и компьютерной информации могут быть со стороны следующих субъектов:

работники фирмы, использующие свое служебное положение (когда законные права по должности используются для незаконных операций с информацией);

работники фирмы, не имеющие права в силу своих служебных обязанностей, но, тем не менее, осуществившими несанкционированный доступ к конфиденциальной информации;

лица, не связанные с фирмой трудовым соглашением (контрактом).

В процессе своей деятельности предприниматели, неоднократно испытывающие неправомерные действия других субъектов, не всегда обращаются в правоохранительные органы, либо вообще стараются не разглашать случаи посягательств на их компьютерные системы. Это связано с тем, что фирмы, коммерческие банки не хотят “отпугнуть” клиентов, потребителей тем фактом, что их компьютерные системы (а значит и вся информация, содержащаяся в них) недостаточно хорошо защищены. Латентная по своему характеру преступность приносит наибольший вред, поскольку безнаказанность преступников позволяет им продолжать и расширять свою преступную деятельность.

# Глава 3

Обеспечение безопасности предпринимательской деятельности со стороны компьютерных систем представляет собой один из блоков проблемы безопасности вообще. Защита от компьютерных преступлений должна начинаться с разработки концепции информационной безопасности фирмы. На основе вышеназванных принципов – вероятности угрозы, возможности защиты и экономической целесообразности защиты информации разрабатываются конкретные способы защиты.

Способы защиты можно разделить на две группы – организационные и технические. Организационные способы защиты связаны с ограничением возможного несанкционированного физического доступа к компьютерным системам. Технические способы защиты предполагают использование средств программно-технического характера, направленных, прежде всего, на ограничение доступа пользователя, работающего с компьютерными системами фирмы, к той информации, обращаться к которой он не имеет права (подробнее о программно-технических и технических средствах обеспечения информационной безопасности см. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. Справочник. – М.: Новый Юрист, 1998, с. 189-238).

Специалисты-практики выделяют, например, такие основные направления технической защиты компьютерной системы:

защита информационных ресурсов от несанкционированного доступа и использования – используются средства контроля включения питания и загрузки программного обеспечения, а также методы парольной защиты при входе в систему;

защита от утечки по побочным каналам электромагнитных излучений и наводок – с помощью экранирования аппаратуры, помещений, применением маскирующих генераторов шумов, дополнительной проверкой аппаратуры на наличие компрометирующих излучений;

защита информации в каналах связи и узлах коммутации – используются процедуры аутентификации абонентов и сообщений, шифрование и специальные протоколы связи;

защита юридической значимости электронных документов – при доверительных отношениях двух субъектов предпринимательской деятельности и когда возникает необходимость передачи документов (платежных поручений, контрактов) по компьютерным сетям - для определения истинности отправителя документ дополняется “цифровой подписью” – специальной меткой, неразрывно логически связанной с текстом и формируемой с помощью секретного криптографического ключа;

защита автоматизированных систем от компьютерных вирусов и незаконной модификации – применяются иммуностойкие программы и механизмы модификации фактов программного обеспечения.

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
| **Фамилия ученика** | **Русский язык** | **Математика** | **Информатика** |
| Иванов | Отлично | Хорошо | Хорошо |
| Петров | Хорошо | Отлично | Удовлетворительно |
| Яшин | Хорошо | Удовлетворительно | Отлично |
| Кудрев | Отлично | Хорошо | Отлично |
| Зайцева | Отлично | Хорошо | Хорошо |
| Мишина | Удовлетворительно | Отлично | Хорошо |

Действенным способом ограничения несанкционированного доступа к компьютерным системам является также регулярная смена паролей, особенно при увольнении работников, обладающих информацией о способах защиты.

Основные понятия:

* **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
* **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
* **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Многие современные люди даже не знают о том, что представляют собой основы компьютерной безопасности. Для большинства рядовых пользователей компьютерная безопасность представляет собой что-то вроде ограничения своего компьютера от возможных атак со стороны хакеров. Но в действительности же это гораздо более обширное понятие, в которое входит достаточно большое количество компонентов. В первую очередь, нужно правильно понимать, что основы компьютерной безопасности – это не только антивирусы, это еще и большое количество работ, направленных на то, чтобы ваш компьютер внезапно не перестал работать, а вы не потеряли всю нужную вам информацию. Основы компьютерной безопасности (общие понятия) Именно по этой причине любому пользователю важно знать хотя бы теоретические основы компьютерной безопасности для того, чтобы впоследствии он их мог эффективно использовать на практике. Информационная безопасность основы компьютерной безопасности Как известно, основой работы любого компьютера является информация, которая в XXI веке превратилась уже в полноценный ресурс. В большинстве случаев он гораздо дороже реальных денег. Современный мир всецело основывается на информации, начиная от обычной бытовой жизни и заканчивая военным делом, в котором каждая армия старается развивать преимущественно информированность, а уж затем - военную мощь[[1]](#footnote-1). Именно по этой причине первое и наиболее важное, что включают в себя основы компьютерной безопасности, – информационная безопасность. Что такое информационная безопасность? теоретические основы компьютерной безопасности Основы информационной и компьютерной безопасности представляют собой определенный комплекс мер, направленный на то, чтобы пользователь внезапно не потерял свои данные. Кто-то, услышав термин «информационная безопасность», сразу представляет себе штат правительственных хакеров, которые следят за государственной безопасностью и сохранностью важных для страны данных. Но на самом деле это понятие более обширное, оно охватывает даже обыкновенные бытовые компьютеры. Ведь вряд ли кто-нибудь хочет внезапно увидеть, как фотографии с важных мероприятий, коллекция музыки или же пароли от различных аккаунтов внезапно пропали без возможности восстановления.

Довольно популярной в современных вузах стала компьютерная безопасность (специальность). На нее поступает очень много абитуриентов по всей России. Только вот ближе к концу обучения многие задумываются над тем, кем же они должны работать. И именно этот момент зачастую приносит множество неприятностей. Тем не менее сегодня мы с вами попытаемся разобраться, какая карьера "светит" выпускникам компьютерной безопасности. На практике многие уверяют, что это направление многогранно - вы сможете работать там, где только пожелаете. Но так ли это? Мы постараемся ответить на данный вопрос.

(1)

Компьютерная безопасность специальность Инженер Специальность 10.05.01 (компьютерная безопасность), как правило, подразумевает подготовку студентов-инженеров. То есть вы легко и просто сможете устроиться на данную должность. Но далеко не каждый выпускник хочет работать самым настоящим инженером. В большинстве случаев свободных вакансий много, а вот заработная плата мала. Особенно если сравнить ее с возлагаемой ответственностью, а также обязанностями и рабочим графиком. Зачастую школьников заманивают специальностью, обещая к выпуску престижную работу, но на деле все получается немного иначе. Именно по этой причине некоторые абитуриенты сначала пытаются ответить на вопрос: "Компьютерная безопасность [[2]](#footnote-2)(специальность) - что это такое?" Но однозначного ответа они не получают и решаются своими глазами увидеть, с чем им придется иметь дело. И если должность инженера вам не по вкусу, то давайте думать дальше, что может подойти для построения собственной карьеры. Работа в школе Очень интересная специальность - "Компьютерная безопасность". Вузы, где преподают ее, обычно умалчивают о том, что с трудоустройством у выпускников могут возникнуть определенные проблемы. И вместо обещанных "золотых гор", придется устраиваться хоть куда-нибудь. Лишь бы зарабатывать. компьютерная безопасность специальность вузы Например, в школу. Очень часто выпускники данного направления устраиваются работать самыми обычными учителями информатики. И получают за это копейки. Лишь в престижных школах можно действительно достойно зарабатывать. Но об этом, как правило, говорить в вузах не принято. Вот такая неоднозначная "компьютерная безопасность" (специальность). Образовательная программа данного направления дает, если честно, поверхностные знания по многим направлениям, которые в дальнейшем влияют на трудоустройство каждого выпускника. Куда же еще можно пойти работать кроме инженерии и школ? Оператор связи Специальность "Компьютерная безопасность" отзывы от выпускников получает довольно неоднозначные. Особенно когда вопрос встает о трудоустройстве по выпуску. Почему так получается? Кто-то может найти себе тепленькое местечко, а кто-то - нет. Тем не менее некоторые выпускники стараются устроиться работать оператором связи. Или, иными словами, монтажником к какому-нибудь интернет-провайдеру. Там вам гарантируют стабильный заработок и престижную работу. Правда, с графиком все сложнее - он нестабилен. Например, при определенные сбоях и авариях вы рискуете потерять законный выходной. Зато сама по себе работа у операторов в большинстве случаев не пыльная. Исправить неполадки на линии (для профессионала это не проблема), подключить клиентам оборудование или настроить его — вот то, что придется делать. Вот такая многосторонняя "компьютерная безопасность" (специальность). Вузы, где ее преподают, встречаются везде и всюду. В России вы можете обнаружить данное направление во всех высших учебных заведениях, специализирующихся на информатике и математике. Но это далеко не все популярные вакансии среди выпускников специальности. Куда еще устраиваются?

1. Военная мощь, достижимая при предельном напряжении материальных... [↑](#footnote-ref-1)
2. Компьютерная безопасность - это защита данных на вашем компьютере от различных случайных или намеренных удалений данных с локальных дисков. [↑](#footnote-ref-2)