**МИНИСТЕРСТВО НАУКИ**



**И ВЫСШЕГО ОБРАЗОВАНИЯ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО**

**ОБРАЗОВАНИЯ**

**ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ**

**УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ**

**Кафедра Информационной безопасности**

**РЕФЕРАТ**

**по ­­­­­­­­­­­­­­­­­­­­­** Основам информационной безопасности

**на тему «Понятие защиты информации и режима секретности. Меры по обеспечению режима конфиденциальности»**

**АВТОР РАБОТЫ** В.М.Розенберг, 16.11.2022 **ГРУППА** УБ-11

ИНИЦИАЛЫ, ФАМИЛИЯ, ДАТА

**СПЕЦИАЛЬНОСТЬ**  10.05.03 Информационная безопасность

НАИМЕНОВАНИЕ

**ШИФР**  217187

ЗАЧЕТНОЙ КНИЖКИ № ВАРИАНТА



**РАБОТА ЗАЩИЩЕНА**

ДАТА ПОДПИСЬ

**ПРИНЯЛ** В.В. Зиновьева

ПОДПИСЬ ДАТА ИНИЦИАЛЫ ФАМИЛИЯ

**ВОРОНЕЖ 2022 г.**

**СОДЕРЖАНИЕ**

Введение…………………………………………………………….………….....3

1 Понятие защиты информации…………………………………………………4

2 Понятие режима секретности……………….....................................................5

3 Режимы секретности...........................................................................................6

4 Организационные средства защиты информации………………....................8

5 Конфиденциальность………………………...………………………………..10

6 Меры по обеспечению режима конфиденциальности………………………12

7 Уровни защиты информации……………………………………………….…15

Заключение………………………………….………………….……………...…18

Список источников……………………………………….…………………...…19

**ВВЕДЕНИЕ**

Защите важной информации, не подлежащей разглашению, приходится уделять большое внимание как частным лицам, так и многим фирмам. Утечка секретных сведений оборачивается потерей клиентов и снижением доходов. Злоумышленники могут овладеть ценной информацией, нанести урон репутации граждан, получить доступ к банковским счетам, частным и государственным секретным документам. Для защиты конфиденциальной информации, предотвращения ее использования в незаконных или преступных целях используют технические средства.

Проблема защиты информации от несанкционированного доступа к ней возникла давно, с той поры, когда человеку по каким-либо причинам не хотелось делиться ею ни с кем или не с каждым человеком. С развитием человеческого общества, появлением частной собственности, государственного строя, борьбой за власть и дальнейшим расширением масштабов человеческой деятельности информация приобретает цену. Ценной становится та информация, обладание которой позволит ее существующему и потенциальному владельцам получить какой-либо выигрыш: материальный, политический, военный и т.д. С переходом на использование технических средств связи информация подвергается воздействию случайных процессов: неисправностям и сбоям оборудования, ошибкам операторов и т.д., которые могут привести к ее разрушению, изменениям на ложную, а также создать предпосылки к доступу к ней посторонних лиц. С дальнейшим усложнением и широким распространением технических средств связи возросли возможности для преднамеренного доступа к информации.

**1 ПОНЯТИЕ ЗАЩИТЫ ИНФОРМАЦИИ**

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

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий.

Информационная безопасность, как и защита информации, задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем.

**2 ПОНЯТИЕ РЕЖИМА СЕКРЕТНОСТИ**

Режим секретности – совокупность требований, правил, организационных технических мер, направленных на сохранение сведений, составляющих государственную тайну (статья 26 Закона Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне»).

Режим секретности — это установленный нормативными актами единый порядок обеспечения защиты сведений, составляющих государственную тайну, включающий систему административно-правовых, организационных, инженерно-технических и других мер. Таким образом, внутриобъектовый и пропускной режимы являются неотъемлемой частью комплекса мероприятий, направленных на защиту сведений, составляющих государственную тайну, и сохранность их носителей.

**3 РЕЖИМЫ СЕКРЕТНОСТИ**

Режим секретности устанавливает единый порядок в стране. Разрабатывает сведения, составляющие государственную и служебную тайны.

Для них определена цель: предотвратить утечки закрытой информации по агентурным каналам.

Особенности режима секретности:

- контроль за деятельностью по обеспечению сохранности государственных секретов, соблюдение требований установленного режима секретности, который осуществляется органами государственной безопасности;

- порядок выполнения должностными лицами своих должностных обязанностей по сохранению государственных и служебных тайн, по соблюдению режима секретности;

- персональная ответственность руководителей всех рангов за организацию режима секретности в их учреждениях, организациях и предприятиях, за проведение необходимого комплекса мероприятий, предотвращающих утечку закрытой информации;

- единый для всех министерств, ведомств, предприятий, учреждений, организаций порядок обращения с государственными секретами, которые определяются высшими органами государственной власти и управления;

- порядок проведения служебных расследований по фактам разглашения секретных сведений;

- обязательный для всех государственных органов и должностных лиц порядок обращения с государственными секретами;

- порядок установления степени секретности сведений, содержащихся в работах, документах и изделиях;

- порядок обеспечения секретности при осуществлении предприятиями, учреждениями и организациями, где ведутся закрытые работы, контактов с зарубежными фирмами;

- порядок допуска граждан к работам, документам и изделиям, которые содержат закрытую информацию;

- порядок обеспечения секретности при проведении в учреждениях и на предприятиях работ закрытого характера;

- порядок обеспечения секретности при ведении секретного делопроизводства;

- порядок выполнения должностными лицами своих должностных обязанностей по сохранению государственных и служебных тайн, по соблюдению режима секретности;

- порядок обеспечения секретности при использовании технических средств, передаче, обработке и хранении информации закрытого характера.

**4 ОРГАНИЗАЦИОННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ**

В решении задач организационного обеспечения информационной безопасности предприятия важную роль играют организационные средства защиты информации. Под организационными средствами защиты информации понимается комплекс мероприятий, планируемых и осуществляемых в целях организации внутриобъектового режима. Они являются, по сути, связующим звеном между персоналом предприятия и различными техническими и иными средствами, используемыми в целях организации и обеспечения режима секретности. Наиболее эффективны следующие меры по защите информации, относящиеся к организационным средствам защиты информации:

• организация разработки, внедрения и использования различных средств и систем защиты информации;

• организация разработки, размножения, учета и уничтожения носителей конфиденциальной информации с использованием технических средств;

• контроль за соблюдением персоналом предприятия установленных требований при использовании объектов информатизации;

• анализ эффективности функционирования технических систем и средств защиты информации;

• разработка и внедрение в практику инструкций и иных документов, регламентирующих порядок и правила обращения с конфиденциальной информацией.

Порядок организации внутриобъектового режима, задачи, решаемые должностными Лицами и структурными подразделениями предприятия, отражаются в разрабатываемых на предприятии внутренних организационно-распорядительных документах, утверждаемых руководителем предприятия. Сотрудники, в установленном порядке допущенные к информации с ограниченным доступом и осуществляющие непосредственную работу с этой информацией, несут ответственность за соблюдение требований нормативных актов по порядку обращения с носителями конфиденциальной информации и за сохранность этих носителей.

**5 КОНФИДЕНЦИАЛЬНОСТЬ**

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. [ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации»]

Виды конфиденциальной информации:

Конфиденциальная информация, как и государственная тайна, относится к информации ограниченного доступа. Согласно указу Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера», к видам информации конфиденциального характера относятся: персональные данные, коммерческая тайна, служебная тайна, профессиональная тайна.

Термины видов конфиденциальной информации:

Персональные данные — это любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных). ФЗ-152 «О персональных данных» Настоящий закон регулирует деятельность по обработке (использованию) персональных данных.

Коммерческая тайна — это режим конфиденциальности информации, позволяющий ее обладателю увеличить доходы, избежать неоправданных расходов, занять лидирующее положение на рынке или получить коммерческую выгоду.

Служебная тайна — это защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Служебная тайна является видом конфиденциальной информации, и право на служебную тайну выступает самостоятельным объектом права. Проект ФЗ «О служебной тайне» (N 124871-4) Настоящий закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам. ФЗ «Об информации, информатизации и защите информации»

Профессиональная тайна — это защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

**6 МЕРЫ ПО ОБЕСПЕЧЕНИЮ РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ**

Средства защиты секретной информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они препятствуют доступу к информации, в том числе с помощью её маскировки. К аппаратным средствам относятся: генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны — недостаточная гибкость, относительно большие объём и масса, высокая стоимость.

Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки — ограниченная функциональность сети, использование части ресурсовфайл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.

Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки — высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

По степени распространения и доступности выделяются программные средства, другие средства применяются в тех случаях, когда требуется обеспечить дополнительный уровень защиты информации.

Программные средства защиты секретной информации:

* Встроенные средства защиты информации;
* Антивирусная программа (антивирус) — программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом;
* Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства. Кроме программ шифрования криптографических систем, существует много других доступных внешних средств защиты информации;
* Межсетевые экраны (также называемые брандмауэрами или файрволами. Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода — это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой;
* Proxy-servers (proxy — доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью —маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях — например, на уровне приложения (вирусы, код JavaScript);
* VPN (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTPPPPoEIPSec.

**7 УРОВНИ ЗАЩИТЫ ИНФОРМАЦИИ**

Ранее контроль доступа к конфиденциальной информации и защита её от влияний извне был задачей технических администраторов.

Сегодня же защита информации становится обязанностью каждого пользователя системы, что требует не только навыков обращения с системой безопасности, но и знаний о способах неправомерного доступа для предотвращения такового. Надежный контроль над информацией обеспечивает безопасность бизнеса, а также позволяет качественно и своевременно устранять ошибки, возникающие в течение производственных процессов, облегчая работу персонала.

Основные уровни защиты информации на предприятии. Можно выделить три основных уровня защиты информации:

- защита информации на уровне рабочего места пользователя;

- защита информации на уровне подразделения предприятия;

- защита информации на уровне предприятия.

Информация первоначально создается на конкретном рабочем месте рядового пользователя системы предприятия. Очень часто именно там информация хранится и первично обрабатывается.

Рабочие места чаще всего объединяются в локальную сеть для совместной работы и обмена информацией. В данном случае мы говорим о локальной сети подразделения, пользователи которой находятся друг от друга на достаточно небольших расстояниях.

Уровни защиты информации локальной сети подразделения отличаются более сложными механизмами, чем на рабочем месте пользователя. Защита данных на различных уровнях имеет как общие, так и специальные способы защиты.

Локальные сети подразделений часто объединены в общую сеть предприятия, которая кроме рабочих мест рядовых пользователей имеет в своем составе также серверное оборудование и специализированные устройства, которые отвечают за функционирование и защиту всей сети предприятия. Кроме того, локальные сети предприятия могут быть географически удалены друг от друга.

Организация системы безопасности по уровням. В системе безопасности существуют следующие уровни защиты информации:

- физическая защита информации;

- контроль доступа и персональная идентификация;

- применение ключей для шифрования данных;

- защита излучения кабеля;

- защита «обратный вызов».

Для правильного построения защитных механизмов системы безопасности следует изучить не только функционирование информационных потоков внутри предприятия, но и возможности неправомерного доступа к информации извне. В зависимости от типа угрозы, применяются определенные меры по защите информации. Поэтому каждому уровню соответствует тот или иной способ защиты информации.

Уровни защиты, в соответствии с механизмами реагирования на угрозы. В соответствии с механизмами реагирования на угрозу, определяют следующие уровни защиты информации:

- предотвращение – внедрение служб контроля доступа к информации и технологии;

- обнаружение - раннее обнаружение угрозы, даже в случае обхода механизмов защиты;

- ограничение – уменьшение размера информационных потерь, в случае уже произошедшего преступления;

- восстановление - обеспечение эффективного восстановления информации в случае её утраты или уничтожения. Таким образом, существует несколько уровней защиты информации, характеризующиеся применение различных методов и механизмов реагирования.

**ЗАКЛЮЧЕНИЕ**

Подводя итоги, следует упомянуть о том, что известно множество случаев, когда фирмы (не только зарубежные) ведут между собой настоящие «шпионские войны», вербуя сотрудников конкурента с целью получения через них доступа к информации, составляющую коммерческую тайну. Регулирование вопросов, связанных с коммерческой тайной, еще не получило в России достаточного развития. Имеющееся законодательство все же не обеспечивает соответствующего современным реалиям регулирования отдельных вопросов, в том числе и о коммерческой тайне. В то же время надо отдавать себе отчет, что ущерб, причиненный разглашением коммерческой тайны, зачастую имеет весьма значительные размеры (если их вообще можно оценить). Наличие норм об ответственности, в том числе уголовной, может послужить работникам предостережением от нарушений в данной области, поэтому целесообразно подробно проинформировать всех сотрудников о последствиях нарушений. Хотелось бы надеяться, что создающаяся в стране система защиты информации и формирование комплекса мер по ее реализации не приведет к необратимым последствиям на пути зарождающегося в России информационно - интеллектуального объединения со всем миром.

**СПИСОК ИСТОЧНИКОВ**

1 <https://www.it-grad.ru/blog/obrabotka-i-zashhita-personalnyx-dannyx-chasto-zadavaemye-voprosy>

2 <https://www.sesiya.ru>

3 <https://www.miit.ru/content/Обложка.pdf?id_vf=83791>

4 <https://searchinform.ru/resheniya/biznes-zadachi/rabota-s-konfidentsialnoj-informatsiej/organizatsiya-zaschity-konfidentsialnoj-informatsii/>

5 <https://otherreferats.allbest.ru/law/00286670_0.html>

# 6 [Е. Баранова, А. Бабаш "Информационная безопасность и защита информации" 3-е изд. (2016)](https://www.ozon.ru/context/detail/id/136470734/)

# 7 [А. Бабаш, Е. Баранова, Д. Ларин "Информационная безопасность. История защиты информации в России" (2015)](https://www.ozon.ru/context/detail/id/21438682/)