**Содержание:**

# ВВЕДЕНИЕ

Актуальность темы. Несмотря на различия в интерпретациях, определениях и акцентах, представляется целесообразной выработка единообразного подхода к применению понятия "личность" по отношению к субъекту, участвующему в обеспечении информационной безопасности, и определению интересов личности как объекта правового обеспечения информационной безопасности. Представляет немалый научный интерес и вопрос определения правомочий личности в глобальном информационном обществе. Сфера безопасности в информационном обществе, к которой приковано внимание, обусловливает необходимость обеспечения баланса интересов государства, общества и каждой отдельной личности. В условиях информационного общества проблема соотношения и взаимозависимости интересов личности, информационного общества и информационного государства требует взвешенного подхода в решении. Справедливо специалистами в сфере правового обеспечения информационной безопасности отмечается, что «важные элементы информационного общества - это принципы, такие как доверие и безопасность в использовании ИКТ, которые вытекают из необходимости поощрять, развивать и активно внедрять устойчивую глобальную культуру кибербезопасности». Неотъемлемой частью национальной безопасности любой страны в современном мире является информационная безопасность, которая характеризует состояние сохранности общества в информационной сфере.

Цель работы - изучение видов и составов информационной безопасности

Объектом исследования является – информационная безопасность общества.

Предметом исследования является – методы обеспечения информационной безопасности.

Поставлены задачи:

- определить понятие и структуру информационной безопасности;
- изучить виды угроз информационной безопасности;

- проанализировать принципы обеспечения и защиту безопасности в информационной сфере;
- рассмотреть политику информационной безопасности и ее влияние на процесс управления безопасностью;
- охарактеризовать систему информационной безопасности в Российской Федерации.

Теоретическая основа исследования - теоретические исследования, научные концепции и разработки, содержащиеся в публикациях, монографиях таких правоведов, как Б. С. Анисимов, В.А. Балуев, И.В. Баранов, П. Борисов.

Методологическая основа исследования: использованы методы: наблюдения, исследования.

Структура данной работы состоит из введения, двух глав, заключения, списка использованной литературы.

# 1 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – СОХРАННОСТЬ ОБЩЕСТВА В ИНФОРМАЦИОННОЙ СФЕРЕ

## 1.1 Понятие и структура информационной безопасности

Говорят, что информация – это своего рода нефть: ее также сначала недооценивали, однако, роль ее в обществе все росла, что в совокупности с другими факторами (в частности, возрастанием роли информационных и телекоммуникационных технологий) привело к так называемой информационной революции и формирования информационного общества[1].

В современное время информация, ее создание, использование и распространение является основой не только сферы культуры, но и экономики и политики.

Под информационной безопасностью понимается комплекс организационных и технических мер, которые принимаются для обеспечения защиты, целостности, доступности и управляемости массивов информации.

Подписанными международными договорами и соглашениями предусмотрено сотрудничество по развитию информационного общества, а оно вряд ли возможно без обеспечения информационной безопасности, кибербезопасности и конфиденциальности.

Немаловажную роль в обеспечении безопасности компьютерной техники имеют такие факторы, как своевременное сервисное обслуживание, ремонт и установка лицензионного программного оборудования на персональных ПК и ноутбуках, что в значительной мере позволяет обеспечить безопасность компьютерной техники от заражения вирусами, длительную и устойчивую работоспособность[2].

Кибербезопасность это защищенность жизненно важных интересов человека и гражданина, общества и государства в киберпространстве, при которой обеспечиваются устойчивое развитие информационного общества и цифровой коммуникационной среды, своевременное выявление, предотвращение и нейтрализация реальных и потенциальных угроз национальной безопасности страны в киберпространстве. Во-первых, совершенно непонятно, что за «жизненно важные интересы» в киберпространстве, которые защищаются, но это больше вопрос законодательной техники. Во-вторых, это определение дублирует дефиницию «национальной безопасности» с определенным приспособлением к особенностям объекта правовой охраны, а это не совсем правильно, учитывая то, что может сложиться впечатление, что киберпространство – это некая «параллельная реальность». На самом деле это не так, параллельной реальности не существует.

В рамках общей концепции безопасности государства информационная безопасность обеспечивает связанное взаимодействие всех элементов системы.

Структурные элементы информационной безопасности включают[3]:

- защиту сведений, содержащих государственную или коммерческую тайну;
- защиту серверов государственных учреждений и систем жизнеобеспечения;
- защиту безопасности данных как набор аппаратных и программных средств, которые обеспечивают сохранность информации от неавторизированного доступа, затруднения доступа, разрушения и перепрограммирования;
- информационно-психологический блок, который подразумевает реализацию системы мер, направленных на защиту от целенаправленного информационного воздействия на субъект нападения, его психологическое состояние или имидж на международной арене.

Таким образом, защита всех составляющих требует разработки методического аппарата и создания собственной инфраструктуры. Задачи обеспечения информационной безопасности осложняются тем, что информационное пространство не имеет границ.

## 1.2 Виды угроз информационной безопасности

Под «угрозой» в данном контексте подразумевают потенциально возможные действия, явления и процессы, которые способны привести к нежелательным последствиям или воздействиям на операционную систему или на сохраненную в ней информацию. В современном мире известно достаточно большое количество таких информационных угроз, виды которых классифицируют на основании одного из критериев.

Так, по природе возникновения выделяют[4]:

- Естественные угрозы. Это те, которые возникли вследствие физических воздействий или стихийных явлений.
- Искусственные угрозы. К данному виду информационных угроз относятся все, которые связаны с действиями человека.

В зависимости от непосредственного источника угрозы информационной безопасности могут быть природные (например, стихийные явления), человеческие (нарушение конфиденциальности информации путем ее разглашения), программно-аппаратные. Последний вид в свою очередь может разделяться на санкционированные (ошибки в работе операционных систем) и несанкционированные (взлом сайта и заражение вирусами) угрозы.

В зависимости от положения источника выделяют 3 основных вида информационных угроз[5]:

- Угрозы от источника, находящегося за пределами компьютерной операционной системы. Например, перехват информации в момент передачи ее по каналам связи.
- Угрозы, источник которых находится в пределах подконтрольной операционной системы. Например, хищение данных или утечка информации.
- Угрозы, возникшие внутри самой системы. Например, некорректная передача или копирование ресурса.

Вне зависимости от удаленности источника вид информационной угрозы может быть пассивным (воздействие не влечет изменений в структуре данных) и активным (воздействие меняет структуру данных, содержание компьютерной системы).

Кроме того, информационные угрозы могут появиться на этапах доступа к компьютеру и обнаружиться после разрешенного доступа (например, несанкционированное использование данных).

В соответствии с местом расположения в системе виды информационных угроз могут быть 3 типов: те, которые возникают на этапе доступа к информации, расположенной на внешних устройствах памяти, в оперативной памяти и в той, что циркулирует по линиям связи.

Некоторые угрозы (например, хищение информации) не зависят от активности системы, другие (вирусы) обнаруживаются исключительно при обработке данных.

Механизмы реализации данного вида информационных угроз изучены достаточно хорошо, как и методы для их предотвращения.

Особую опасность для компьютерных систем представляют аварии и естественные (стихийные) явления. В результате такого воздействия становится недоступной информация (полностью или частично), она может исказиться или совсем уничтожиться[6]. Система обеспечения информационной безопасности не может полностью исключить или предупредить такие угрозы.

Другая опасность – это допущенные ошибки при разработке компьютерной системы. Например, неверные алгоритмы работы, некорректное программное обеспечение. Именно такие ошибки часто используются злоумышленниками.

Еще один вид непреднамеренных, но существенных видов угроз информационной безопасности – это некомпетентность, небрежность или невнимательность пользователей. В 65% случаев ослабления информационной безопасности систем именно нарушения функциональных обязанностей пользователями приводили к потере, нарушениям конфиденциальности и целостности информации.

Механизмы реализации данного вида информационных угроз изучены достаточно хорошо, как и методы для их предотвращения.

Особую опасность для компьютерных систем представляют аварии и естественные (стихийные) явления. В результате такого воздействия становится недоступной

информация (полностью или частично), она может исказиться или совсем уничтожиться. Система обеспечения информационной безопасности не может полностью исключить или предупредить такие угрозы.

Другая опасность – это допущенные ошибки при разработке компьютерной системы. Например, неверные алгоритмы работы, некорректное программное обеспечение. Именно такие ошибки часто используются злоумышленниками[7].

Преднамеренные информационные угрозы - этот вид угроз характеризуется динамичным характером и постоянным пополнением все новыми видами и способами целенаправленных действий нарушителей.

Вне зависимости от удаленности источника вид информационной угрозы может быть пассивным (воздействие не влечет изменений в структуре данных) и активным (воздействие меняет структуру данных, содержание компьютерной системы).

Кроме того, информационные угрозы могут появиться на этапах доступа к компьютеру и обнаружиться после разрешенного доступа (например, несанкционированное использование данных).

В соответствии с местом расположения в системе виды информационных угроз могут быть 3 типов: те, которые возникают на этапе доступа к информации, расположенной на внешних устройствах памяти, в оперативной памяти и в той, что циркулирует по линиям связи.

Некоторые угрозы (например, хищение информации) не зависят от активности системы, другие (вирусы) обнаруживаются исключительно при обработке данных.

В данной сфере злоумышленники используют специальные программы[8]:

- Вирусы - небольшие программы, которые самостоятельно копируются и распространяются в системе.
- Черви - активирующиеся при каждой загрузке компьютера утилиты. Подобно вирусам, они копируются и самостоятельно распространяются в системе, что приводит к ее перегрузке и блокировке работы.
- Троянские кони - скрытые под полезными приложениями вредоносные программы. Именно они могут пересылать злоумышленнику информационные файлы и разрушать программное обеспечение системы.

Таким образом, вредоносные программы не единственный инструмент преднамеренного вторжения. В ход идут также многочисленные методы шпионажа – прослушка, хищение программ и атрибутов защиты, взлом и хищение документов. Перехват паролей чаще всего производится с использованием специальных программ.

# 2 ЗАЩИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 2.1 Принципы обеспечения и защита безопасности в информационной сфере

Главными принципами информационной безопасности, системы обеспечения ее сохранности и неприкосновенности являются[9]:

- Целостность информационных данных. Этот принцип подразумевает, что информация сохраняет содержание и структуру при ее передаче и хранении. Право на создание, изменение или уничтожение данных сохраняется лишь у пользователей с соответствующим статусом доступа.
- Конфиденциальность данных. Подразумевается, что доступ к массиву данных имеет четко ограниченный круг пользователей, авторизованных в данной системе, тем самым обеспечивая защиту от несанкционированного доступа к информации.
- Доступность массива данных. В соответствии с данным принципом, авторизованные пользователи получают своевременный и беспрепятственный к ней доступ.
- Достоверность информации. Этот принцип выражается в том, что информация строго принадлежит только субъекту, от которого она принята и который является ее источником.

Вопросы информационной безопасности выходят на первый план в случае, если нарушения в работе и возникающие ошибки в компьютерной системе могут привести к серьезным последствиям. И под задачами системы обеспечения информационной безопасности подразумевают многоплановые и комплексные меры. Они включают предотвращение неправомерного использования, повреждения, искажения, копирования и блокирования информации. Сюда относится отслеживание и предотвращение несанкционированного доступа лиц

без должного уровня авторизации, предотвращение утечки информации и всех возможных угроз ее целостности и конфиденциальности. При современном развитии баз, данных вопросы безопасности становятся важными не только для мелких и частных пользователей, но и для финансовых структур, крупных корпораций.

Несмотря на постоянный рост и динамическое развитие различного рода информационных угроз, существуют все же и методы защиты.

- Физическая защита – это первый этап информационной безопасности. Сюда относится ограничение доступа для посторонних пользователей и пропускная система, особенно для доступа в серверное подразделение.
- Базовый уровень защиты информации – это программы, блокирующие компьютерные вирусы и антивирусные программы, системы для фильтрации корреспонденции сомнительного характера.
- Защита от DDoS-атак, которую предлагают разработчики программного обеспечения.
- Создание резервных копий, хранящихся на других внешних носителях или в так называемом «облаке».
- План аварийной работы и восстановления данных. Этот метод важен для крупных компаний, которые хотят обезопасить себя и сократить время простоя в случае сбоя.
- Шифрование данных при передаче их с помощью электронных носителей[10].

Защита информации требует комплексного подхода. И чем большее количество методов будет использоваться, тем эффективнее будет осуществляться защита от несанкционированного доступа, угроз уничтожения или повреждения данных, а также их хищений.

Важной задачей становится обеспечение на должном уровне информационной безопасности в социальной и образовательной сферах. Ярким проявлением отсутствия должных мер защиты является вовлечение несовершеннолетних в опасные сетевые сообщества террористической или суицидальной направленности. Основная причина кроется в недостаточной локализации популярных интернет-ресурсов и невозможность полного контроля с российской стороны над глобальными социальными сетями. В первом случае проблема заключается в том, что принцип давления на крупнейшие ресурсы с требованиями о предоставлении персональных данных пользователей срабатывает не всегда, как в случае с «Твиттером» и «Фейсбуком. Во втором случае требуется координация

различных служб, так как справиться с проблемой только силами МВД и Роскомнадзора невозможно. За 2018 год Роскомнадзор заблокировал 17 тыс. доменных имен и пользователей, но они появляются вновь – под другими именами, но с тем же кругом последователей.

Таким образом, в современном обществе информационных технологий и хранения на электронных носителях огромных баз, данных вопросы обеспечения безопасности информации и видов информационных угроз не лишены праздности. Случайные и преднамеренные действия естественного или искусственного происхождения, которые могут нанести ущерб владельцу или пользователю информацией.

## 2.2 Политика информационной безопасности и ее влияние на процесс управления безопасностью

Защита корпоративных данных обеспечивается путем проведения комплекса мер, направленных на достижение определенного уровня информационной безопасности компании.

Дорожкин А.В. и Ясенев В.Н. отмечают, что концепция обеспечения информационной безопасности предприятия для поддержания экономической безопасности предприятия определяет потенциальные источники угроз информационной безопасности предприятия и меры противодействия им со стороны предприятия и, рассматривая информацию как объект защиты, устанавливает цель и задачи, которые необходимо решить для обеспечения информационной безопасности предприятия[11].

Макеев А.С. отмечает, что процесс управления информационной безопасностью включает в себя 3 уровня: стратегический, тактический и оперативный. На стратегическом уровне происходит общая организация обеспечение интересов предприятия в области безопасности. Здесь формируются стратегия и основные мероприятия по обеспечению информационной безопасности. Также на данном уровне формируется Политика информационной безопасности. На тактическом уровне осуществляется планирование и обеспечение выполнения Политики информационной безопасности. Разрабатываются необходимые регламенты, правила и инструкции. В рамках тактического уровня проводятся расследования и анализ инцидентов информационной безопасности. На уровне оперативного

управления происходит реализация конкретных контрмер, нейтрализующих информационные угрозы.

Далее показано основные шаги обеспечения безопасности:

- Уточнение важности информационных и технологических активов предприятия;
- определения уровня безопасности для каждого актива, а также средства безопасности, которые будут рентабельными для каждого актива
- Определение рисков на угрозы активам;
- Привлечение нужных денежных ресурсов для обеспечения политики безопасности, а также приобретение и настройка нужных средств для безопасности;
- Строгий контроль поэтапной реализации плана безопасности, для выявление текущих просчетов, а также учета изменения внешних факторов с дальнейшим изменением требуемых методов безопасности;
- Проведение объяснительных действий для персонала и остальным ответственным сотрудникам.

Следующие требования к политикам безопасности составлены на ряде ошибок и проб большинства организаций:

Политики безопасности должны[12]:

- указывать на причины и цели создания политики безопасности;
- осматривать, какие границы и ресурсы охватываются политикой безопасности;
- определить ответственных по политике безопасности;
- определить условие не выполнение и так званное наказание
- политики безопасности должны быть реальными и осуществимыми;
- политики безопасности должны быть доступными, краткими и однозначными для понимания;
- должна быть золотая середина между защитой и производительностью;

Основные шаги по разработке политики есть:

- создание адекватной команды для создание политики;
- решить вопросы об возникающих особенностях при разработки.
- решить вопросы об области действии и цели создании политики;
- решить вопросы по поводу ответственных за создания и выполнения данного документа;

Нужно проанализировать локальную сеть на локальные атаки. Сделав основные шаги нужно проанализировать есть ли выход локальной сети (seti_PDH или seti_dwdm) в интернет. Ведь при выходе сети в интернет возникает вопрос о проблемах защиты информации в сетях. Потом какие компьютеры и сетевые сервисы используются уже в сети. Определить количество сотрудников по ряду критерию. К примеру, скольким нужен доступ в интернет, сколько пользуется электронной почтой и другими онлайн сервисами. Также определить есть ли удаленный доступ к внутренней сети.

После проведения анализа и систематизации информации, команде нужно перейти к анализу и оценки рисков. Анализ рисков — это самый важный этап формирования политики безопасности.

На этом этапе реализуются следующие шаги[13]:

- анализ угроз информационной безопасности которые непосредственно обозначены для объекта защиты;
- оценка и идентификация цены информационных и технологических активов;
- осмотр вероятности реализации угроз на практике;
- осмотр рисков на активы.

После осмотра рисков на активы нужно переходить к установке уровня безопасности, который определяет защиты для каждого актива. Есть правило, что цена защиты актива не должна превышать цены самого актива.

*Пример подхода компании Sun Microsystems.*

Специалисты Sun считают, что политика есть необходимой для эффективной организации режима информационной безопасности предприятия. Они же под политикой безопасности подразумевают стратегический документ, в котором описаны требования и ожидания руководства предприятии. Они рекомендуют создать подход сверху-вниз, сначала создать политику безопасности, а потом уже строить архитектуру информационной системы.

К созданию политики безопасности они рекомендуют завлечь таких сотрудников подразделений как:

- управление бизнесом;
- отдел защиты информации;
- техническое управление;

- департамент управления рисками;
- отдел системного/сетевого администрирования;
- юридический отдел;
- департамент системных операций;
- отдел кадров;
- служба внутреннего качества и аудита.

Основной назначение политики безопасности — информирование руководство и сотрудников компании от текущих требованиях о защите данных в информационной системе.

Идея политики безопасности к основным идеям относят[14]:

- назначения ценности информационных активов;
- управление остаточными рисками; $R = H \times P$, где H — оценка ущерба, P — вероятность угрозы.
- управление информационной безопасностью;
- обоснованное доверие.

Принцип безопасности — это первый шаг при создании политики, к ним относят:

- Ознакомления — участники информационной системы обязаны быть ознакомлены о требованиях политики безопасности и о ответственности.
- Ответственность — ложится на каждого пользователя за все его действия в информационной сети.
- Этика — деятельность сотрудников компании должна быть в соответствии со стандартами этики.
- Комплексность — должны учитываться все направления безопасности.
- Экономическая оправданность — все действия развитии предприятия должны быть экономически оправданными.
- Интеграция — все направления политики, процедур или стандартов должны быть интегрированы и скоординированы между собой.
- Своевременность — все противодействия угрозам должны быть своевременны.
- Демократичность — все действия по защите активов на предприятии должны быть в нормах демократии.
- Аккредитация и сертификация — компания и все ее действия должны быть сертифицированы
- Разделение привилегий — все права сотрудников должны быть разделены относительно их допуска к ресурсам.

## 2.3 Система информационной безопасности в Российской Федерации

В современное время, когда можно с уверенностью сказать, что Россия перешла от постиндустриального к информационному обществу, остро встает проблема создания высокоэффективной системы информационной безопасности. Чтобы разобраться в данном вопросе следует обозначить следующие определения.

Информация – эта совокупность данных, которые передаются людьми всеми возможными способами, как письменно, так и устно, а также с помощью иных специфических знаков.

Безопасность – это состояние защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз.

Информационная безопасность – совокупности мероприятий по сохранению целостности информации, а также обеспечение безопасности передачи, хранения и других видов деятельности с информацией.

Исходя из предложенных определений, можно представить масштабы системы, которая на уровне государства должна обеспечивать информационную безопасность.

Фундамент современной системы информационной безопасности составляет Доктрина информационной безопасности Российской Федерации, которая была принята президентом в 2000 году[15]. С того времени ведется активная работа по развитию данной системы. В результате работы был разработан целый ряд нормативно-правовых актов, составляющих основу рассматриваемой системы. Организованна деятельность, направленная на создание «машины», реализующей взаимодействие объектов общества в информационной сфере[16].

В основу системы информационной безопасности легли сами причины появления системы – угрозы информационной безопасности, то есть условия и факторы, которые создают ситуацию опасности. Субъектами данной системы являются как все государство и общество в целом, так и отдельный гражданин. Объектом же считается информационная сфера, принадлежащая субъектам. Особую роль в системе играет политика государства в сфере информационной безопасности, которая является отражением принятых решений и реальных мер,

предпринимаемых органами власти.

Система информационной безопасности РФ касается всех ветвей власти: законодательной, исполнительной и судебной. Данную систему наиболее четко можно представить в схеме (рис.1)

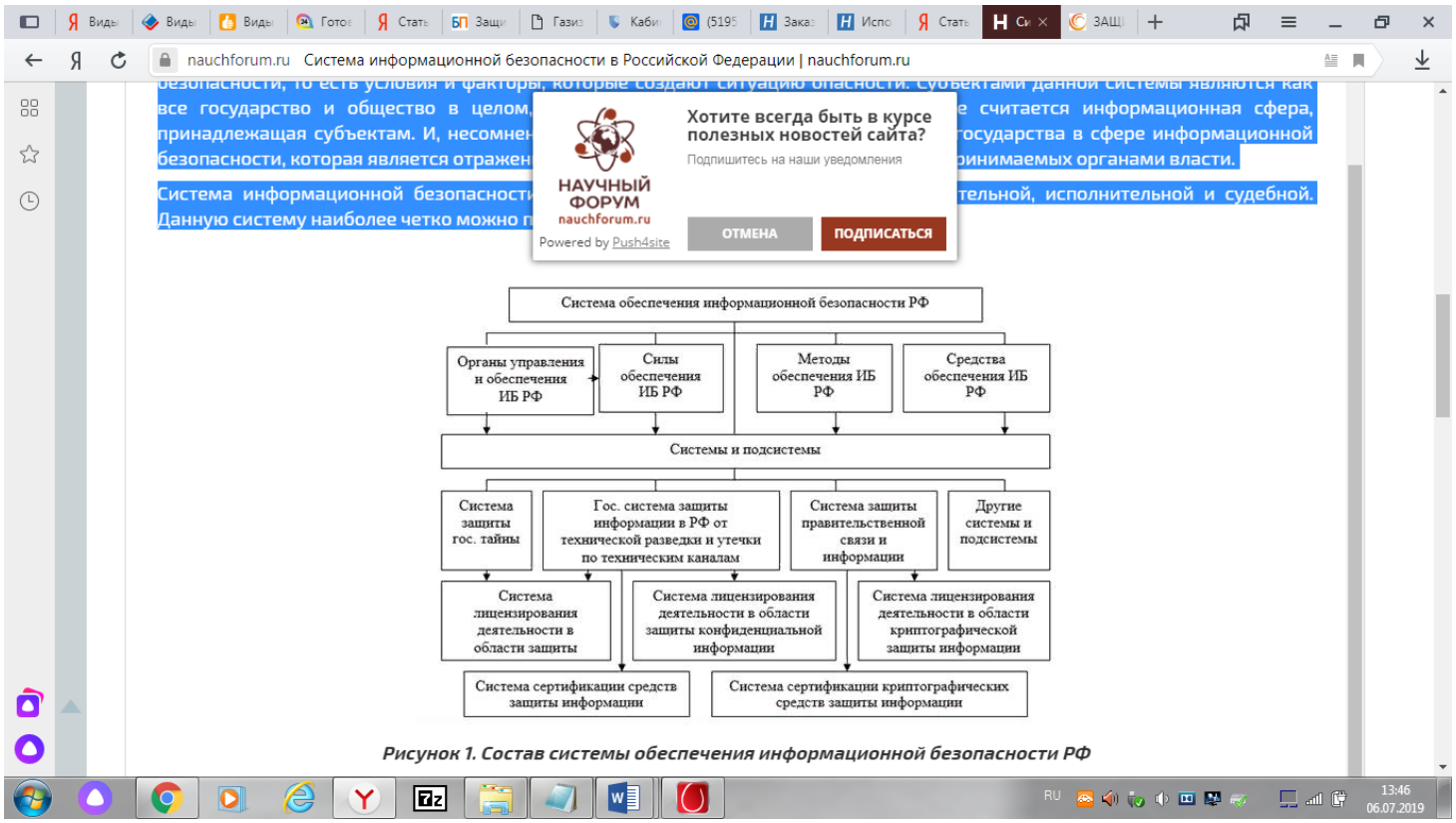


*Рис. 1. Состав системы обеспечения информационной безопасности РФ[17]*

Органы управления и обеспечения информационной безопасности представляют собой «фундамент» системы обеспечения информационной безопасности. Их так же можно представить в виде схемы (рис.2).

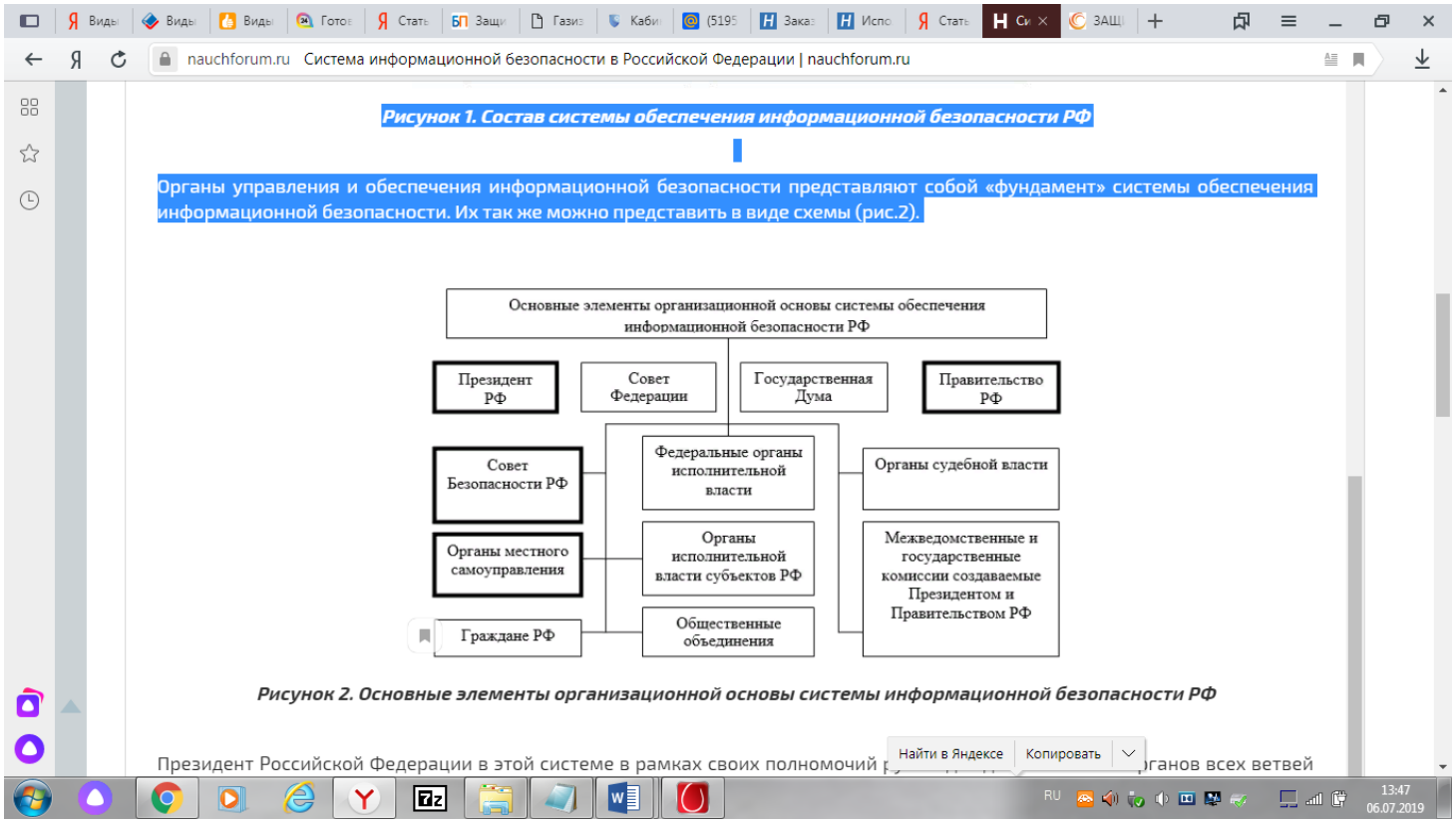


*Рис. 2. Основные элементы организационной основы системы информационной безопасности РФ[18]*

Президент Российской Федерации в этой системе в рамках своих полномочий руководит деятельностью органов всех ветвей власти, вводит санкции и дает разрешения на действия, направленные на реализацию работы системы обеспечения информационной безопасности, а также начиная с 2000 года. В ежегодном послании отражены желаемые направления развития мер защиты данных.

Следующим элементом является Правительство РФ, которое, учитывая сформулированные в ежегодном послании Президента РФ приоритетные направления в сфере обеспечения информационной безопасности, контролирует деятельность органов исполнительной власти, как на федеральном уровне, так и на уровне субъектов. Правительство следит за выделением средств из федерального бюджета, которые будут направлены на обеспечения сохранности информации.

Немаловажным элементом в данной системе является Совет Федерации, который осуществляет деятельность, связанную с выявлением и оценкой возможных угроз информационной безопасности Российской Федерации, разрабатывает меры по

предотвращению воздействия угроз по отношению к информации, устанавливает контроль над органами, ответственными за работу данной системы, а также оперативно реагирует на возникновение опасности нарушения, повреждения или потери данных[19].

Обеспечением исполнения законодательства Российской Федерации, а также иных нормативно-правовых актов в сфере информационной безопасности занимаются федеральные органы исполнительной власти.

Согласно рисунка 2 расположены органы исполнительной власти субъектов Российской Федерации, которые, взаимодействуя с федеральными органами, выполняют те же функции на местном уровне, а также вносят предложения по совершенствованию системы органов обеспечения информационной безопасности в вышестоящие органы.

Органы судебной власти выполняют функцию осуществления правосудия по отношению к нарушителям системы обеспечения информационной безопасности.

Межведомственные и государственные комиссии, которые создаются Президентом и Правительством РФ, обладают определенными четко установленными полномочиями в сфере обеспечения гарантии безопасности данных.

К силам обеспечения информационной безопасности Российской Федерации относятся органы исполнительной власти, в полномочия которых входит выполнение задач, гарантирующих сохранность информационной базы.

К таким органам причисляют[20]:

- Федеральная служба обеспечения информации (ФСОБ).
- Служба внешней разведки Российской Федерации (СВР).
- Государственная техническая комиссия при Президенте Российской Федерации.
- Федеральное агентство правительственной связи и информации (ФАПСИ).
- Министерство внутренних дел Российской Федерации.
- Различные органы судебной власти.
- Государственный таможенный комитет Российской Федерации.
- Госстандарт Российской Федерации.

Методы и средства обеспечения информационной безопасности вытекают из причины угрозы, полномочного органа, занимающегося данным вопросом.

Далее в системе обеспечения информационной безопасности следуют подсистемы, специализирующиеся на узких направлениях, таких как защита государственной тайны, защита правительственной связи и информации и т.д.

Таким образом, на сегодняшний день в Российской Федерации сформирована полная, четкая, взаимосвязанная система информационной безопасности. Необходимо продолжить работу в данном направлении, совершенствуя систему и подстраивая её под изменяющиеся условия. Следует активизировать и совершенствовать международно-правовое сотрудничество в сфере предупреждения и борьбы с компьютерными преступлениями. Учитывая транснациональный и трансграничный характер рассматриваемых преступлений, большое значение приобретает вопрос взаимодействия правоохранительных органов России и зарубежных стран в сфере противодействия компьютерной преступности. Обеспечение информационной безопасности России носит комплексный характер, что требует эффективного взаимодействия прокуратуры, органов безопасности и других правоохранительных органов с институтами гражданского общества.

# ЗАКЛЮЧЕНИЕ

Информационная безопасность (ИБ) – это состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц. Безопасность данных также подразумевает управление рисками, которые связаны с разглашением информации или влиянием на аппаратные и программные модули защиты.

Кибербезопасность это защищенность жизненно важных интересов человека и гражданина, общества и государства в киберпространстве, при которой обеспечиваются устойчивое развитие информационного общества и цифровой коммуникационной среды, своевременное выявление, предотвращение и нейтрализация реальных и потенциальных угроз национальной безопасности страны в киберпространстве.

Структурные элементы информационной безопасности включают:

- защиту сведений, содержащих государственную или коммерческую тайну;
- защиту серверов государственных учреждений и систем жизнеобеспечения;

- защиту безопасности данных как набор аппаратных и программных средств, которые обеспечивают сохранность информации от неавторизированного доступа, затруднения доступа, разрушения и перепрограммирования.

Выделяют:

- Естественные угрозы. Это те, которые возникли вследствие физических воздействий или стихийных явлений.
- Искусственные угрозы. К данному виду информационных угроз относятся все, которые связаны с действиями человека.

В соответствии со степенью преднамеренности угрозы подразделяются на случайные и преднамеренные.

В зависимости от непосредственного источника угрозы информационной безопасности могут быть природные (например, стихийные явления), человеческие (нарушение конфиденциальности информации путем ее разглашения), программно-аппаратные.

Главными принципами информационной безопасности, системы обеспечения ее сохранности и неприкосновенности являются:

- Целостность информационных данных.
- Конфиденциальность данных.
- Доступность массива данных.
- Достоверность информации.

Таким образом, защита информации требует комплексного подхода. И чем большее количество методов будет использоваться, тем эффективнее будет осуществляться защита от несанкционированного доступа, угроз уничтожения или повреждения данных, а также их хищений. Информационная безопасность сегодня все больше и больше становится актуальной темой в информационном обществе. Задача каждого человека — постараться обеспечить максимально эффективную защиту информации. Так как в современном обществе именно информация имеет очень важную роль.

# СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 05.12.2016 г. № 646. – [Электронный ресурс] – Режим доступа. –URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 10.05.18).
2. Алексейчева, Е.Ю. Экономика организации (предприятия): Учебник для бакалавров / Е.Ю. Алексейчева, М.Д. Магомедов. - М.: Дашков и К, 2016. - 292 с.
3. Асаул В.В. Обеспечение информационной безопасности в условиях формирования цифровой экономики // В.В. Асаул. Теория и практика сервиса: экономика, социальная сфера, технологии, 2018. №4 (38). –54 с.
4. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.
5. Евдокимов К.Н. Сравнительно-правовой анализ законодательства России и зарубежных стран, регламентирующего уголовную ответственность за совершение компьютерных преступлений // Юридический мир. 2017. № 3. С. 45-49.
6. Информационные системы и технологии: Научное издание. / Под ред. Ю.Ф. Тельнова. - М.: ЮНИТИ, 2016. - 303 с.
7. Коноплева, И.А. Информационные технологии. / И.А. Коноплева, О.А. Хохлова, А.В. Денисов. - М.: Проспект, 2015. - 328 с.
8. Корнеев, И.К. Информационные технологии в работе с документами: Учебник / И.К. Корнеев. - М.: Проспект, 2015. - 304 с.
9. Косиненко, Н.С. Информационные системы и технологии в экономике: Учебное пособие / Н.С. Косиненко, И.Г. Фризен. - М.: Дашков и К, 2015. - 304 с.
10. Минзов А.С. Информационная безопасность в цифровой экономике //А.С. Минзов. ИТНОУ: информационные технологии в науке, образовании и управлении, 2018. №3 (7). - 23 с.
11. Мамонова, Т.Е. Информационные технологии. лабораторный практикум: Учебное пособие для прикладного бакалавриата / Т.Е. Мамонова. - Люберцы: Юрайт, 2016. - 176 с.
12. Мельников, В.П. Защита информации: Учебник / В.П. Мельников. - М.: Академия, 2019. - 320 с.
13. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с
14. Советов, Б.Я. Информационные технологии: учебник для прикладного бакалавриата / Б.Я. Советов, В.В. Цехановский. - Люберцы: Юрайт, 2016. - 263 с.

15. Северин, В.А. Правовая защита информации в коммерческих организациях: Учебное пособие / В.А. Северин. - М.: Академия, 2019. - 656 с.
16. Сергеев, И.В. экономика организации (предприятия): Учебник и практикум для прикладного бакалавриата / И.В. Сергеев, И.И. Веретенникова. - Люберцы: Юрайт, 2015. - 511 с.
17. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРА-М, 2017. - 304 с.
18. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2018. - 352 с.
19. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. - М.: ДМК Пресс, 2017. - 275 с.
20. Ярочкин, В. Безопасность информационных систем / В. Ярочкин. - М.: Ось-89, 2016. - 320 с.

1. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 30 с. ↑

2. Мамонова, Т.Е. Информационные технологии. лабораторный практикум: Учебное пособие для прикладного бакалавриата / Т.Е. Мамонова. - Люберцы: Юрайт, 2016. - 43 с. ↑

3. Советов, Б.Я. Информационные технологии: учебник для прикладного бакалавриата / Б.Я. Советов, В.В. Цехановский. - Люберцы: Юрайт, 2016. - 73 с. ↑

4. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 22с ↑

5. Коноплева, И.А. Информационные технологии. / И.А. Коноплева, О.А. Хохлова, А.В. Денисов. - М.: Проспект, 2015. - 22 с. ↑

6. Северин, В.А. Правовая защита информации в коммерческих организациях: Учебное пособие / В.А. Северин. - М.: Академия, 2019. - 81 с. ↑

7. Минзов А.С. Информационная безопасность в цифровой экономике //А.С. Минзов. ИТНОУ: информационные технологии в науке, образовании и управлении, 2018. №3 (7). - 13 с. ↑

8. Мельников, В.П. Защита информации: Учебник / В.П. Мельников. - М.: Академия, 2019. - 10 с. ↑

9. Косиненко, Н.С. Информационные системы и технологии в экономике: Учебное пособие / Н.С. Косиненко, И.Г. Фризен. - М.: Дашков и К, 2015. - 54 с. ↑

10. Сергеев, И.В. экономика организации (предприятия): Учебник и практикум для прикладного бакалавриата / И.В. Сергеев, И.И. Веретенникова. - Люберцы: Юрайт, 2015. - 51 с. ↑

11. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРА-М, 2017. - 304 с. ↑

12. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2018. - 65 с. ↑

13. Ярочкин, В. Безопасность информационных систем / В. Ярочкин. - М.: Ось-89, 2016. - 54 с. ↑

14. Асаул В.В. Обеспечение информационной безопасности в условиях формирования цифровой экономики // В.В. Асаул. Теория и практика сервиса: экономика, социальная сфера, технологии, 2018. №4 (38). –14 с. ↑

15. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 05.12.2016 г. № 646. – [Электронный ресурс] – Режим доступа. –URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 10.05.18). ↑

16. Евдокимов К.Н. Сравнительно-правовой анализ законодательства России и зарубежных стран, регламентирующего уголовную ответственность за

совершение компьютерных преступлений // Юридический мир. 2017. № 3. С. 46. ↑

17. Корнеев, И.К. Информационные технологии в работе с документами: Учебник / И.К. Корнеев. - М.: Проспект, 2015. - 24 с. ↑

18. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. - М.: ДМК Пресс, 2017. - 25 с. ↑

19. Алексейчева, Е.Ю. Экономика организации (предприятия): Учебник для бакалавров / Е.Ю. Алексейчева, М.Д. Магомедов. - М.: Дашков и К, 2016. - 83 с. ↑

20. Информационные системы и технологии: Научное издание. / Под ред. Ю.Ф. Тельнова. - М.: ЮНИТИ, 2016. - 36 с. ↑