

# Введение в ИБ

Основы информационной  
безопасности



# Оглавление

Введение.....	4
Словарь терминов.....	4
Актуальность обеспечения ИБ.....	5
Информация как актив и категории защищаемой информации.....	6
Ключевые понятия и концепции обеспечения ИБ, а также их взаимосвязи.....	8
<b>Конфиденциальность, целостность и доступность (англ. CIA).....</b>	<b>9</b>
<b>Аутентификация, авторизация и учёт (англ. AAA).....</b>	<b>10</b>
<b>Циклы PDCA и OODA.....</b>	<b>10</b>
<b>Концепция «Защита в глубину» (Defense in depth).....</b>	<b>11</b>
<b>Концепция «Нулевое доверие» (Zero Trust).....</b>	<b>12</b>
<b>Основные принципы и методы обеспечения ИБ.....</b>	<b>12</b>
Нормативно-правовое и методическое обеспечения, ключевые регуляторы в области обеспечения ИБ.....	13
<b>Обеспечение безопасности персональных данных.....</b>	<b>14</b>
<b>Обеспечение безопасности критической информационной инфраструктуры Российской Федерации.....</b>	<b>15</b>
<b>Обеспечение защиты информации при осуществлении банковской деятельности и деятельности в сфере финансовых рынков.....</b>	<b>16</b>
<b>Охрана конфиденциальности информации, составляющей коммерческую тайну.....</b>	<b>17</b>
<b>Международное законодательства по линии ИБ.....</b>	<b>18</b>
<b>Заключение по блоку нормативно-правового и методического обеспечения... </b>	<b>18</b>
Ответственность и этические принципы в областях обеспечения и нарушения ИБ.	19

Специализации в области обеспечения ИБ.....	20
Выводы.....	20
Дополнительные материалы.....	21
Использованная литература.....	21

# Введение

Сегодня мы начнём курс, посвященный основам обеспечения информационной безопасности (ИБ), а первое занятие - введение в данную тематику.

Для начала давайте познакомимся: меня зовут Александр Кузнецов, и с GeekBrains я сотрудничаю с 2019 года. Вне GeekBrains я руковожу группой архитектуры в крупнейшем коммерческом центре мониторинга ИБ – JSOC «Ростелеком-Солар», и отвечаю за построение таких центров в российских и зарубежных компаниях.

За свою профессиональную деятельность я выполнил сотни проектов, в т.ч. провёл первые в России практические киберучения для крупного банка, участвовал в составе международной команды по построению крупнейшего центра мониторинга ИБ в России, а также выступал ключевым автором методических рекомендаций по категорированию объектов критической информационной инфраструктуры для операторов связи.

Являюсь держателем профильных международных статусов CISM и CISSP, а также кандидатом технических наук по специальности ИБ.

Основная задача нашего курса – это дать вам необходимую базу для самостоятельного решения первоочередных задач по обеспечению ИБ в повседневной деятельности, а также для взаимодействия с вашими коллегами из служб информационной безопасности.

## На этой лекции вы узнаете:

- Почему сегодня крайне актуальна тематика обеспечения ИБ?
- Почему информация представляет из себя важный актив, и какие бывают категории защищаемой информации?
- Какие есть ключевые понятия и концепции обеспечения ИБ?
- Какое нормативно-правовое и методическое обеспечения, а также ключевые регуляторы есть в данной области?
- Что можно сказать об ответственности и этических принципы в областях обеспечения и нарушения ИБ?
- Какие есть специализации в области обеспечения ИБ?

## Словарь терминов

Несмотря на то, что это вводная лекция и затрагивает многие аспекты обеспечения ИБ, в части терминологии здесь будут даны только самые первоочередные понятия, а уже на последующих занятиях планомерно добавятся все остальные термины и определения.

**Информация** – сведения (сообщения, данные) независимо от формы их представления ([Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»](#)).

**Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств ([Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»](#)).

**Информационная безопасность организации** – состояние защищенности интересов организации в условиях угроз в информационной сфере ([ГОСТ Р 53114-2008](#)).

**Обеспечение информационной безопасности организации** – деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности организации или на минимизацию ущерба от возможной реализации таких угроз ([ГОСТ Р 53114-2008](#)).

**Защита информации** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию ([ГОСТ Р 50922-2006](#)).

**Безопасность информации [данных]** – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность ([ГОСТ Р 50922-2006](#)).

**Компьютерная атака (кибератака)** – целенаправленное воздействие программных и/или программно-аппаратных средств на информационные системы (сети передачи данных), в целях нарушения и/или прекращения их функционирования и/или создания угрозы безопасности обрабатываемой ими информации (адаптировано из [Федерального закона от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»](#)).

## Актуальность обеспечения ИБ

На сегодняшний день, с одной стороны, мы наблюдаем:

- рост количества цифровой информации
- рост количества информационных систем и веб-сайтов
- рост количества пользователей сети Интернет и социальных сетей
- рост количества устройств, подключённых к сети Интернет, включая Интернет вещей (Internet of Things)

а с другой:

- рост количества кибератак
- рост ущерба от успешных реализаций кибератак
- появление новой сферы вооруженной борьбы – киберпространство
- рост количества регуляторных требований к обеспечению ИБ (Compliance)

Фактически, это пример *классической противоречивой ситуации*, когда стремительное развитие и распространение информационных технологий, иногда говорят – информационно-коммуникационных технологий, создаёт новые угрозы как отдельным гражданам (пользователям) и организациям, так и целым странам (угрозы национальной безопасности). Например, стратегия национальной безопасности РФ предусматривает обеспечение ИБ страны как неотъемлемую часть нацбезопасности [1].

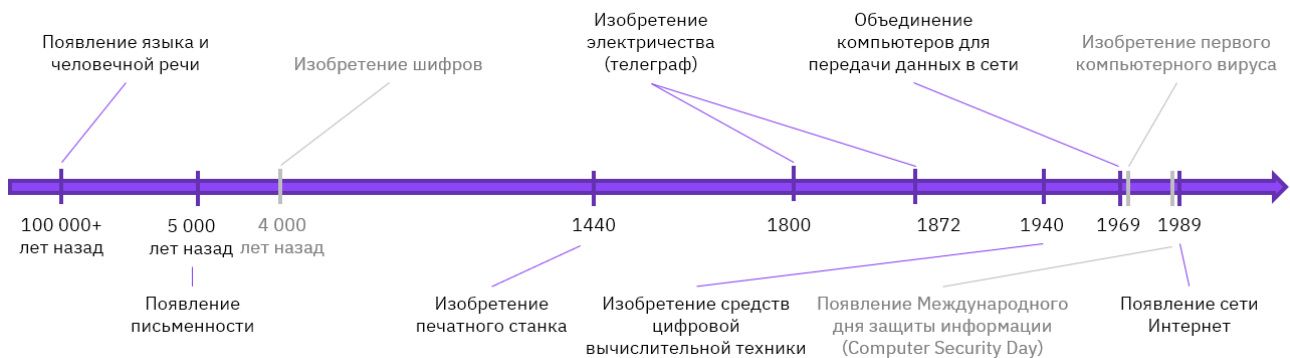
Как следствие, любая организация или отдельный пользователь в любой момент времени может быть подвержен как массовой, так и целенаправленной кибератаке. И нам нужно понимать, как к этому подготовиться, и что каждый из нас может и должен в этой части делать, а чего делать не должен.

Специалисты по ИБ входят в ТОП одних из самых востребованных и высокооплачиваемых в ИТ-сфере, службы ИБ существуют практически в каждой организации, а дисциплины, связанные с ИБ, появляются всё в большем количестве учебных заведений, и GeekBrains не является исключением.

## **Информация как актив и категории защищаемой информации**

Чтобы понять, почему сегодня информация представляет из себя один из важнейших активов для организаций, предлагается посмотреть на историю так называемых *информационных революций*. Они представляли собой резкое преобразование общественных отношений из-за кардинальных изменений в сфере обработки информации.

## Информационные революции



Последняя такая революция – появление сети Интернет, знаменует возникновение фактически безбумажного и отвязанного от физического местонахождения человека – виртуального этапа общественных взаимоотношений. Для данного этапа цифровая информация и сети передачи данных – это «кровеносная система», непрерывно насыщающая организации и граждан. Как следствие, информация – это один из важнейших активов (ценностей) для современных организаций. Часть организаций в принципе строят свой бизнес на сборе, анализе и предоставлении информации через сеть Интернет – маркетплейсы, агрегаторы, Social Media Marketing и т.п.

Информация может быть представлена в самых различных формах, мы продолжим рассмотрение именно цифровой информации (данных) вне зависимости от содержимого (текст, графика, музыка и т.д.), формата и объёма (целая база данных, отдельный файл или единичное сообщение).

В части состояния и локализации местонахождения информации (данных) можно выделить три состояния:

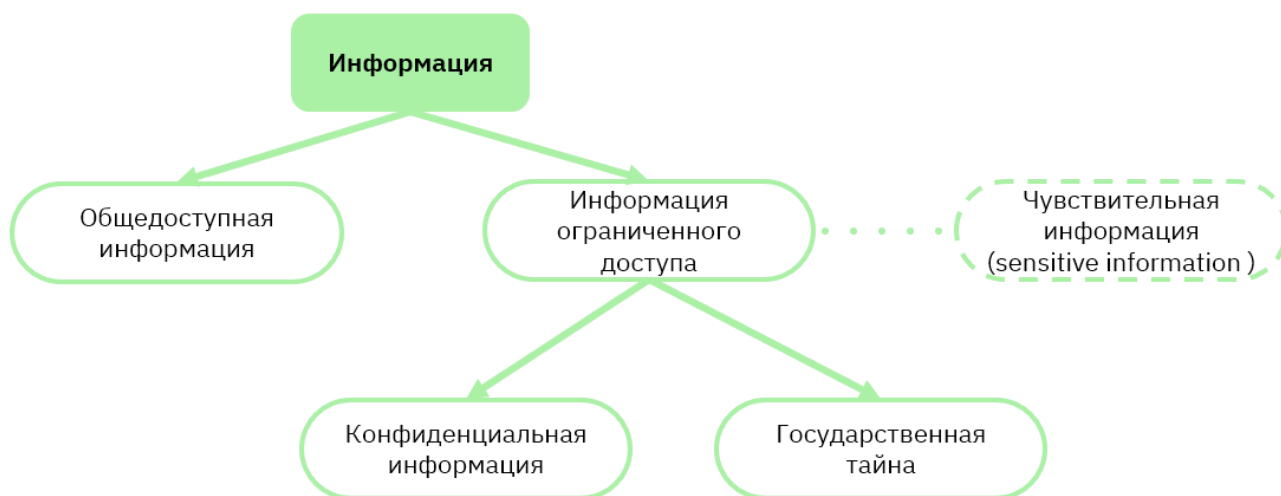
- данные в покое (Data at rest) – данные, хранящиеся на различных носителях
- данные в движении (Data in motion) – данные, передаваемые по сети (сетевой трафик)
- используемые данные (Data in use) – данные, используемые в моменте различными приложениями, в т.ч. находящиеся в оперативной памяти компьютеров

В соответствии с действующим федеральным законодательством [2] в зависимости от категории доступа выделяют:

- общедоступную информацию

- информацию, доступ к которой ограничен федеральными законами (информацию ограниченного доступа):
  - конфиденциальную информацию (например, персональные данные)
  - государственную тайну

В связи с тем, что конфиденциальная информация подразумевает, что она подлежит защите в соответствии с законодательством Российской Федерации, иногда вы можете столкнуться с понятием *чувствительной информации*, на которую нет явных законодательных требований, но есть желание её защищать у конкретной организации (например, схемы сети организации, реквизиты доступа к информационным системам).



💡 Говоря о категориях доступа к информации, не стоит забывать о реализации принципа **«need-to-know»**: положено знать только то, что связано с профессиональной необходимостью. Он позволит правильно ограничить доступ к любым видам информации (данных).

Информацию обрабатывают с использованием различных информационных систем, которые в разрезе ИБ условно можно разделить на следующие ключевые группы:

- информационные системы персональных данных, присутствующие у любых организаций (например, любая кадровая система или система с клиентской базой)
- государственные информационные системы (муниципальные информационные системы), созданные на основании федеральных законов, законов субъектов Российской Федерации или правовых актов



государственных органов, органов местного самоуправления (например, Единый портал государственных и муниципальных услуг)

- объекты критической информационной инфраструктуры, включающие в себя информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления (например, биллинговые системы у операторов связи)

Понимая, к какой группе относится ваша информационная система, можно определить область нормативно-правового регулирования и государственного контроля (надзора) со стороны регуляторов. О них мы поговорим чуть позже.

## Ключевые понятия и концепции обеспечения ИБ, а также их взаимосвязи

Стоит начать с того, что, к сожалению, в области ИБ нет единой терминологии. Существует первичная *кусочная* терминология на уровне различных федеральных законов, несколько *разрозненных* государственных стандартов, посвященных именно «Терминам и определениям», плюс есть отдельные глоссарии на веб-сайтах регуляторов и лидеров ИБ-отрасли (например, [ИТ-энциклопедия «Касперского»](#) и [Энциклопедия кибербезопасности «Ростелеком-Солар»](#)), не говоря уже об учебной и научно-популярной литературе.

В рамках данного курса мы будем придерживаться следующего варианта: понятие *информационной безопасности* будет применяться к чему-то, например: к организации, к системе или т.п. И в таком случае *ИБ организации* – это состояние защищенности интересов организации в условиях угроз в информационной сфере, а *обеспечение ИБ организации* – это соответствующая деятельность для достижения и поддержания данного состояния.

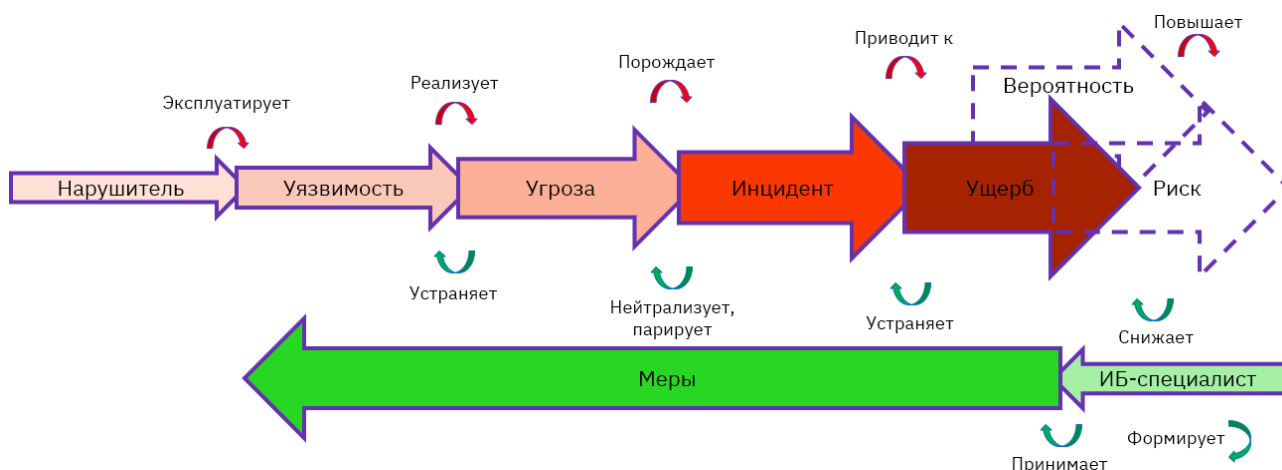
Очень частое сопутствующее ИБ словосочетание *защита информации*, воспринимается его синонимом, но это не совсем так. *Защита информации* – это скорее синоним обеспечению ИБ организации, т.к. это тоже деятельность, а не состояние.

А вот *безопасность информации [данных]* – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

🔥 Таким образом, правильнее уточнять, какой именно терминологический аппарат по линии ИБ используется в конкретной организации, проекте или ситуации, чтобы избежать недопониманий и разночтений с коллегами.

Если посмотреть на терминологию с точки зрения атакующего (нарушителя) и защищающегося (ИБ-специалиста), то получаются следующие цепочки взаимосвязанных понятий:

- нарушитель эксплуатирует уязвимость(и), чтобы реализовать угрозу(ы), реализованная угроза порождает инцидент(ы), который может привести к ущербу (например, временным и/или финансовым потерям организации)
- ИБ-специалист в свою очередь принимает меры, которые снижают ущерб, устраняют инциденты, нейтрализуют угрозы и устраняют уязвимости



Если мы добавим к ущербу вероятность, то перейдём к понятию *риска ИБ* – вероятности (возможности) того, что данная угроза сможет воспользоваться уязвимостью и тем самым нанесёт ущерб организации.

Теперь рассмотрим несколько популярных сущностей и концепций.

## Конфиденциальность, целостность и доступность (англ. CIA)

Это условные *три кита* в мире ИБ, а именно, это ключевые свойства информации (данных), которые нужно обеспечить в рамках их защиты:

- конфиденциальность – возможен только санкционированный доступ к данным (есть разрешение на доступ)

- целостность – возможно только санкционированное изменение данных (есть разрешение на изменения)
- доступность – возможно получить данные в нужное время, если, конечно, доступ санкционирован



Стоит отметить, что в разных ситуациях приоритет у этих свойств может быть разный. Например, у резервных копий приоритетнее целостность, у клиентских данных – конфиденциальность, а у списка товаров на веб-сайте – доступность.

На практике для каждого информационного актива или массива информации выставляются требуемые свойства – КЦД. Это мы попробуем с вами на семинаре.

## Аутентификация, авторизация и учёт (англ. AAA)

Ещё одна популярная ИБ-триада, говорящая о том, что любой пользователь должен проходить подтверждение подлинности – аутентификацию, получать необходимые права и полномочия – авторизацию, и все его действия должны учитываться (вестись журналы аудита событий).

На практике данный набор механизмов защиты информации является минимальным для любой информационной системы или отдельного приложения.

## Циклы PDCA и OODA

Это наиболее популярные циклы реализации мер обеспечения ИБ, а точнее построения и поддержания систем обеспечения (управления) ИБ:

- **PDCA:** Plan, Do, Check, Act
- **OODA:** Observe, Orient, Decide, Act

В первом случае, это классический цикл непрерывного совершенствования из популярных международных стандартов ISO 9 000 серии и 27 000 серии:

- планирование – моделирование угроз, выбор необходимых организационных и технических мер, назначение ответственных лиц, формирование планов и бюджетов на реализацию
- реализация – внедрение организационных и технических мер (например, ввод в действие регламентов, установка и настройка средств защиты информации)

- контроль – периодическое проведение аудитов ИБ, тестирований на проникновения (pentest) и т.п., а местами и непрерывный контроль
- совершенствование – внесение изменений по результатам контроля

Во втором случае, это концепция, предложенная американским полковником Джоном Бойдом (иногда говорят – петля Бойда):

- наблюдение – сбор информации об угрозах и текущих условиях
- ориентация – формирование инструкций для отдельных мероприятий или ситуаций, сведение их в общий план
- принятие решения о реализации плана (выбор плана)
- действие – реализация выбранного плана



Стоит обратить внимание, что это именно непрерывные циклы, т.е. обеспечение ИБ организации – это непрерывный процесс, а не разовое мероприятие или продукт.

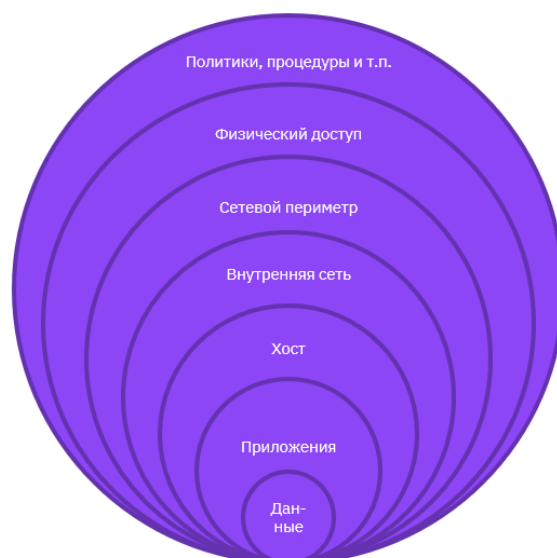
## Концепция «Защита в глубину» (Defense in Depth)

Защита в глубину – это одна из самых популярных и первичных концепций построения систем обеспечения ИБ. Иногда её ещё называют *эшелонированной защитой*. Она берёт свою основу из классической обороны в рамках вооружённых конфликтов.

Принцип реализации – это формирование нескольких, чем больше, тем лучше, уровней защиты (оборонительных линий), которые затрудняют продвижение атакующего извне к цели, в нашем случае – к информации (данным).

Таковыми оборонительными линиями могут выступать самые разные меры защиты, технологии и инструменты, например: турникеты и дверные замки на уровне физического доступа; периметровые межсетевые экраны (firewall) на уровне сетевого периметра; VLAN-сегменты сети на уровне локальной сети; запрос логина и пароля к операционной системе на уровне хоста и т.д.

Фактически это напоминает луковицу или матрёшку:



## Концепция «Нулевое доверие» (Zero Trust)

Достаточно новая концепция (2010 год), но активно набирающая свою популярность. Её основной посыл – «никогда не доверяй, всегда проверяй».

В рамках неё считается, что атакующие действуют как снаружи, так и внутри сети организации. Как следствие, коммуникации должны быть защищены независимо от местонахождения сети (точки подключения к сети), а доступ к ресурсам должен предоставляться только на один сеанс с учётом условий текущего подключения.

Для предоставления доступа рекомендуется руководствоваться двумя принципами:

- **«just-in-time access»**: решение о доступе принимается в момент запроса доступа
- **«just enough access»**: предоставляется лишь такой доступ, который позволяет выполнить задачу

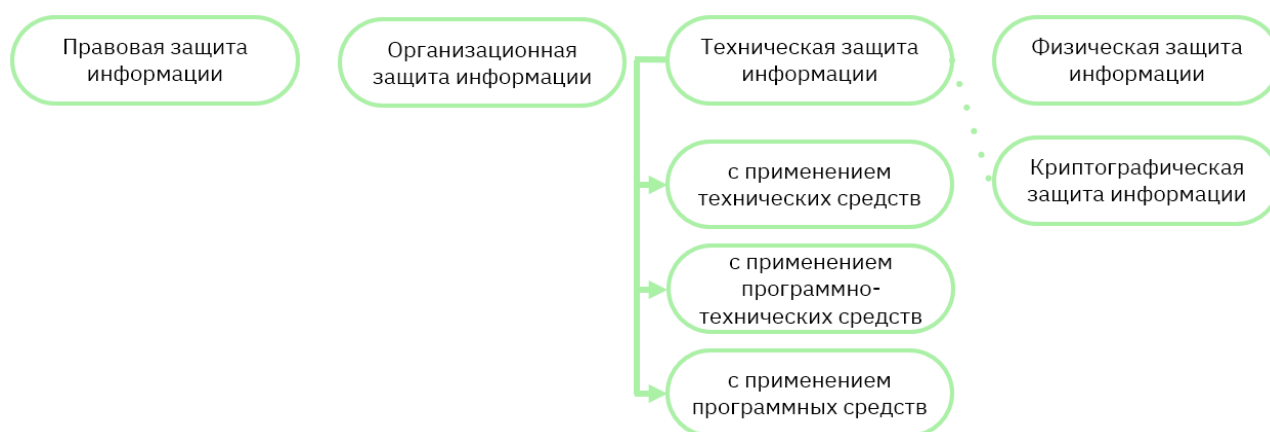
## Основные принципы и методы обеспечения ИБ

Вне зависимости от используемого терминологического аппарата и выбранной концепции на практике применяются следующие основные принципы обеспечения ИБ:

- открытость алгоритмов и механизмов защиты – знание алгоритмов и механизмов не должно давать атакующему возможности преодоления построенных на базе них систем обеспечения ИБ

- законность – любые применяемые мероприятия по обеспечению ИБ не должны противоречить действующему законодательству
- системность – проводимые мероприятия по обеспечению ИБ должны укладываться в единое целое с учётом той концепции, которая была выбрана организацией
- непрерывность – мероприятия по обеспечению ИБ должны проводиться на всех этапах жизненного цикла информационных систем, начиная с формирования требований и заканчивая выводом из эксплуатации
- разумная достаточность – проводимые мероприятия по обеспечению ИБ должны быть соразмерны с защищаемой информацией, потенциальным ущербом и учитывать актуальные угрозы, т.е. условно не стоит строить бункер вокруг школьного компьютера

Существующие методы защиты информации представлены на схеме ниже.



**Правовая защита информации** включает в себя разработку нормативно-правовых документов, фактически реализуется силами различных регуляторов.

**Организационная защита информации** предусматривают установление режимных ограничений, введение в действие и доведение до работников локальных нормативных актов организации.

**Техническая защита информации** предусматривают использование различных технических, программных и программно-технических средств. Иногда явно указывают, что это достигается некриптографическими методами, тогда криптографическую защиту информации выносят в отдельную группу, хотя на практике это всё же составная часть технической защиты информации.

**Физическая защита информации** предусматривают применение средств, создающих препятствия для проникновения или доступа к объекту (на территории, к зданию (сооружению), помещению и т.д.).

Чем больше методов доступно конкретной организации, тем комплекснее (всенаправленнее) может быть организована защита информации.

## **Нормативно-правовое и методическое обеспечения, ключевые регуляторы в области обеспечения ИБ**

В нашей стране сложная иерархия нормативно-правового регулирования, плюс к этому существует большое количество регуляторов по линии ИБ, но ключевыми являются:

- Федеральная служба по техническому и экспортному контролю (ФСТЭК России), для которой основная область регулирования: обеспечение безопасности информации (некриптографическими методами)
- Федеральная служба безопасности (ФСБ России), для которой основная область регулирования: обеспечение ИБ с использованием инженерно-технических и криптографических средств

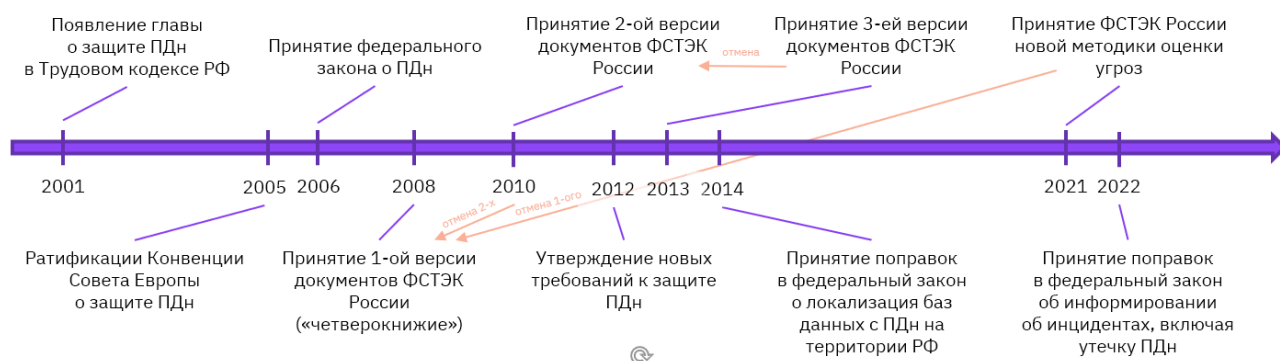
С точки зрения областей нормативно-правового регулирования можно выделить следующие ключевые области:

- обеспечение безопасности персональных данных
- обеспечение безопасности критической информационной инфраструктуры Российской Федерации
- обеспечение защиты информации при осуществлении банковской деятельности и деятельности в сфере финансовых рынков
- охрана конфиденциальности информации, составляющей коммерческую тайну

### **Обеспечение безопасности персональных данных**

Это одна из первых в России и самая масштабная область регулирования, которая переживала несколько «перезапусков», смену акцентов и требований по обеспечению безопасности данных.

## Краткая история правовой защиты ПДн



Несмотря на свой «возраст» и масштабы в данной области существует несколько серьёзных сложностей:

- «размытое» понятие *персональных данных* (ПДн) – это любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту ПДн). И, к сожалению, отсутствует нормативно зафиксированный минимальный и достаточный набор данных, который позволит однозначно определить субъекта ПДн. Здесь нужно следить за актуальными разъяснениями регулятора в лице Роскомнадзора. Например, фамилия, имя, отчество, сведения о состоянии здоровья и т.п. являются ПДн, а вот отдельный номер телефона не является ПДн
- федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» [3] регулирует отношения, связанные с обработкой ПДн, и направлен на защиту прав и свобод человека и гражданина, а не на защиту данных. Как следствие, основные задачи организации и риски (штрафы и т.п.) лежат в области корректной обработки ПДн, а не защиты информации
- учёт требований трёх разных регуляторов: Роскомнадзор, ФСТЭК России и ФСБ России, которые периодически меняются

Установлено четыре уровня защищённости ПДн при их обработке в информационной системе, где 1-ый самый требовательный, а 4-ый менее требовательный.

Комплекс применяемых мер по обеспечению безопасности ПДн представляет собой систему защиты ПДн (СЗПДн). Применяемые средства защиты информации (некриптографические) могут быть несертифицированными ФСТЭК России.



# Обеспечение безопасности критической информационной инфраструктуры Российской Федерации

Это одна из самых «свежих» областей регулирования (2018 г.) – отношения в области обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации в целях её устойчивого функционирования при проведении в отношении неё компьютерных атак. В данной области сделан акцент на практическую *реальную* безопасность различных систем, необходимость которой стала особенно острой после эпидемий вирусов-шифровальщиков в 2017 году.

Действия Федерального закона от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [4] распространяются на 13 сфер:

- здравоохранение
- наука
- транспорт
- связь
- энергетика
- банковская сфера и иные финансовые сферы
- топливно-энергетический комплекс
- область атомной энергии
- оборонная промышленность
- ракетно-космическая промышленность
- горнодобывающая промышленность
- металлургическая промышленность
- химическая промышленность

В данной области присутствует два основных регулятора ФСТЭК России и ФСБ России, при этом отдельными полномочиями наделён Центральный банк Российской Федерации.

Установлено четыре градации объектов КИИ, где 1-ая категория значимости – самая высокая, а 3-ья – самая низкая, а также есть объекты КИИ без категории значимости.

Комплекс применяемых мер, направленных на обеспечение ИБ субъектов КИИ, представляет собой систему безопасности значимых объектов КИИ (СБ ЗОКИИ). Применяемые средства защиты информации (некриптографические) могут быть как сертифицированными ФСТЭК России, так несертифицированными, но прошедшими оценку соответствия в форме испытаний или приёмки.

Информировать Национальный координационный центр по компьютерным инцидентам (НКЦКИ) о компьютерных инцидентах на объектах КИИ обязаны все субъекты КИИ. За счёт этого взаимодействия на уровне страны стараются достигнуть своевременного информационного обмена об угрозах и кибератаках. Для этого же создана Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

## **Обеспечение защиты информации при осуществлении банковской деятельности и деятельности в сфере финансовых рынков**

В отличие от рассмотренных выше областей регулирования здесь ключевым регулятором является не ФСТЭК России и не ФСБ России, а Центральный банк Российской Федерации.

Полномочия Центрального банка Российской Федерации распространяются на следующие типы организаций:

- кредитные организации финансовые организации (банки)
- некредитные финансовые организации (ломбарды, страховые и т.п.)
- субъекты национальной платежной системы

Ещё интересна данная область тем, что существует серия государственных стандартов «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций», которую Центральный банк Российской Федерации через свои нормативные акты сделал обязательными.

Установлено три уровня защиты информации, где 1-ый – усиленный, а 3-ий – минимальный.

Комплекс применяемых мер защиты информации представляет собой систему защиты информации (СЗИ). Применяемые средства защиты информации

(некриптографические) для нейтрализации актуальных угроз должны быть сертифицированными ФСТЭК России.


## **Охрана конфиденциальности информации, составляющей коммерческую тайну**

Последняя область регулирования, которую мы рассмотрим, будет – охрана конфиденциальности информации, составляющей коммерческую тайну.

Интересна и отличительна она следующим:

- может быть релевантна для любого индивидуального предпринимателя или юридического лица
- является добровольной (в отличие от областей, рассмотренных выше)
- явно оперирует одним свойством защищаемой информации – конфиденциальностью

Для начала нужно понять, что *информация, составляющая коммерческую тайну*, – это сведения любого характера (производственные, технические, экономические, организационные и другие), которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам (конкурентам).

 Очень часто для краткости защищаемую информацию называют коммерческой тайной, но это неправильно. Коммерческая тайна – это режим, устанавливаемый в организации, а защищаемая информация – это информация, составляющая коммерческую тайну.

При этом стоит отметить, что режим коммерческой тайны не может быть установлен в отношении некоторых сведений, определённых в Федеральном законе от 29.07.2004 N 98-ФЗ «О коммерческой тайне» [5] (например, содержащихся в учредительных документах, о состоянии противопожарной безопасности, санитарно-эпидемиологической и т.п., о нарушениях законодательства и других).

Меры по охране конфиденциальности информации включают в себя:

- определение перечня информации, составляющей коммерческую тайну
- ограничение доступа к информации, составляющей коммерческую тайну
- учёт лиц, получивших доступ к информации, составляющей коммерческую тайну

- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров
- нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации

Применяемые средства защиты информации (некриптографические) могут быть несертифицированными ФСТЭК России.

## Международное законодательства по линии ИБ

С точки зрения популярного международного законодательства по линии ИБ стоит отметить:

- Payment Card Industry Data Security Standard (PCI DSS): всё что связано с обработкой данных платёжных карт как в банках и процессинговых центрах, так и в торгово-сервисных организациях
- General Data Protection Regulation (GDPR): всё что связано с обработкой ПДн граждан Евросоюза или на территории Евросоюза
- Sarbanes-Oxley Act (SOX): отчётность для организаций, торгующих на американской фондовой бирже (котирующимся на открытом рынке США)

Здесь же стоит затронуть вопросы обеспечения приватности (*privacy*), которые набирают обороты в международном правовом поле и местами перевешивают вопросы обеспечения безопасности.

Если рассмотреть *конфиденциальность* – как обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя, то *приватность* – это право человека полагаться на то, что другие будут надлежащим образом и уважительно использовать, хранить, делиться и распоряжаться связанной с ним персональной и чувствительной информацией в контексте и в соответствии с целями, для которых она была собрана или получена.



## **Заключение по блоку нормативно-правового и методического обеспечения**

- Отсутствует официальный маппинг нормативно-правовых и методических актов между собой. Есть как пересечения, так и расхождения, и противоречия
- Необходимо оценивать применимость (область действия) конкретных нормативно-правовых и методических актов к деятельности конкретной организации
- Необходимо отслеживать статус и изменения релевантных к деятельности конкретной организации нормативно-правовых и методических актов
- Необходимо вовлекать юристов в анализ и работу с нормативно-правовыми и методическими актами

## **Ответственность и этические принципы в областях обеспечения и нарушения ИБ**

На сегодняшний день предусмотрены различные виды ответственности за нарушения в области ИБ:

- дисциплинарная (замечание, выговор или увольнение)
- гражданско-правовая (возмещение убытков и компенсация морального вреда)
- административная (предупреждение или административный штраф)
- Уголовная (штраф или обязательные работы, или исправительные работы, или принудительные работы, или лишение свободы, в т.ч. с лишением права занимать определённые должности)

За несоблюдение (нарушение) требований к обеспечению ИБ предусмотрена как административная, так и уголовная ответственность. Речь о соблюдении

работниками правил, установленных законодательством и организацией-работодателем.

За неправомерные (несанкционированные) действия в отношении защищаемых информационных систем и информации предусмотрена как административная, так и уголовная ответственность. Речь о действиях атакующих (хакеров и т.п.).

Можно выделить следующие этические принципы в области обеспечения ИБ:

- сохранять приватность и конфиденциальность информации, полученной в ходе своей деятельности
- поддерживать компетентность и соглашаться выполнять только ту деятельность, на которую есть необходимые компетенции
- не подвергать опасности своими действиями (бездействиями) жизни и здоровье людей
- развивать и защищать профессию
- не связывать свою деятельность с вредоносными (несанкционированными) и противоправными (противозаконными) активностями
- авторизовывать все действия по анализу (контролю) защищённости
- соблюдать лицензионные (сублицензионные) и иные соглашения / правила использования информационных систем и программного обеспечения, а также различных сервисов

Этические принципы в области ИБ выступают общепринятыми в деловом ИБ-мире ориентирами поведения и сотрудничества. В случае вступления в различные профессиональные ассоциации от кандидата требуется явного принятия соответствующих этических кодексов [6-8].

## **Специализации в области обеспечения ИБ**

На сегодняшний день условно можно выделить следующие специализации в области обеспечения ИБ:

- сетевая безопасность (network security): обеспечение безопасности локальных и распределённых сетей; работа с межсетевыми экранами (FW), системами обнаружения/предотвращения вторжений (IDS/IPS), системами анализа сетевого трафика (NTA), криптошлюзами и другими решениями
- веб-безопасность (web application security): обеспечение безопасности публичных и локальных веб-ресурсов; работа с межсетевыми экранами для веб-приложений (WAF), системами Anti-DDoS и другими решениями

- тестирование на проникновение (penetration testing): контроль и анализ защищённости сетей, информационных систем или отдельных приложений; поиск и эксплуатация уязвимостей (условно «белый хакер» или «красная команда»)
- мониторинг и реагирование на инциденты ИБ (SOC analytics): обнаружение, реагирование и расследование инцидентов ИБ; работа с системами мониторинга (SIEM), систем управления инцидентами ИБ (IRP/SOAR) и другими решениями (условно «синяя команда»)
- аудит и compliance: подготовка и/или проверка организаций на соответствие различным требованиям к обеспечению ИБ
- DevSecOps: координация и автоматизация взаимодействия разработчиков и системных администраторов, а также ИБ-специалистов

Каждая специализация предусматривает свой технический background, свои карьерные лестницы (например, от инженеров до архитекторов или от специалистов до менеджеров) и имеет своих целевых работодателей.

Стоит отметить, что возможно развитие как во внутренней безопасности отдельной организации – in-house, так и в сфере ИБ-услуг – консалтинг и интеграция.

## Выводы

- Обеспечение ИБ крайне актуальное и развивающееся направление как в России, так и за её пределами
- Информация сегодня – это один из важнейших активов организаций, и его нужно защищать
- Существуют различные концепции и методы обеспечения ИБ, имеющие свои достоинства и недостатки
- Нормативно-правовое и методическое обеспечения в области обеспечения ИБ многогранно и разнообразно, нужно быть готовым собирать «свой пазл»
- Предусмотрена различная ответственность за нарушения ИБ как административная, так и уголовная
- Существует профессиональная этика, по которой в т.ч. материалы данного курса не должны быть использованы для нанесения ущерба каким-либо системам, сетям, пользователям и/или организациям
- Существуют различные специализации в области обеспечения ИБ.  
Вы можете выбрать свой вектор дальнейшего карьерного развития, а GeekBrains с этим поможет

## Дополнительные материалы

1. Перечень нормативно-правовых актов, относящих информацию к категории ограниченного доступа: [Справочная информация КонсультантПлюс](#).
2. Книга «Секреты и ложь. Безопасность данных в цифровом мире», Брюс Шнайер, 2003.
3. Новостной telegram-канал: [t.me/true\\_secator](https://t.me/true_secator).
4. Статья «[Цикл Деминга, или PDCA: улучшение процессов разработки и управление качеством продукта](#)», Мария Ираидина.
5. Статья «[Использование цикла OODA в методике SCRUM](#)».

## Использованная литература

1. [Указ Президента РФ от 02.07.2021 N 400 «О Стратегии национальной безопасности Российской Федерации»](#).
2. [Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»](#).
3. [Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»](#).
4. [Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»](#).
5. [Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»](#).
6. [Этический кодекс ISACA](#).
7. [Этический кодекс \(ISC\)<sup>2</sup>](#).
8. [Этический кодекс EC-Council](#).