1. [Информация и информационная безопасность.](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1" \l "p11)

**Информация** (лат. informatio — разъяснение, изложение), первоначально — сведения, передаваемые людьми устным, письменным или другим способом с помощью условных сигналов, технических средств и т.д. С середины 20-го века информация является общенаучным понятием, включающим в себя:

- сведения, передаваемые между людьми;

- сигналы в животном и растительном мире;

- признаки, передаваемые от клетки к клетке, от организма к организму;

- и т.д.

**Защита информации** – комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах.

**Информационная безопасность** – это одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным состоянием (уровнем) защищенности, а защита информации – это процесс, который должен выполняться непрерывно на всем протяжении жизненного цикла информационной системы.

Под **субъектами** информационных отношений понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры.

**Информационная угроза** – потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере, искажению или разглашению информации.

**Политика информационной безопасности** (ПИБ) организации или учреждения – совокупность правил, процедур, практических методов, руководящих принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.

**Объект** – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

**Субъект** – активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

1. [Основные составляющие информационной безопасности.](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1#p12)

Можно выделить следующие составляющие: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

**Доступность информации** – свойство системы обеспечивать своевременный беспрепятственный доступ правомочных (авторизованных) субъектов к интересующей их информации или осуществлять своевременный информационный обмен между ними. Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

**Целостность информации** – свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению. Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций4)). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений. Целостность оказывается важнейшим аспектом информационной безопасности в тех случаях, когда информация служит «руководством к действию». Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным.

**Конфиденциальность информации** – свойство информации быть известной и доступной только правомочным субъектам системы (пользователям, программам, процессам). Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Самый главный вывод, который можно сделать - Информационная безопасность не сводится исключительно к защите от НСД к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от НСД, но и от поломки системы, вызвавшей перерыв в работе.

1. [Категории и носители информации.](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1#p14)

Неотъемлемой частью любой информационной системы является информация. По характеру ограничений (реализации) конституционных прав и свобод в информационной сфере выделяют четыре основных вида правовой (регламентированной законами) информации:

- информация с ограниченным доступом;

- информация без права ограничения;

- иная общедоступная информация (например, за деньги);

- информация, запрещенная к распространению.

Информация с ограниченным доступом делится на государственную тайну и конфиденциальную.

К государственной тайне относятся защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. Владельцем государственной тайны является само государство.

**Конфиденциальная информация** – документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности.

Под персональными данными понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Несмотря на то, что это информация ограниченного доступа, она является полностью открытой для субъекта персональных данных. Только сам субъект решает вопрос о передаче, обработке и использовании своих персональных данных, а также определяет круг субъектов, которым эти данные могут быть сообщены.

**Информация, запрещенная к распространению**, определена в многочисленных нормативных документах. В частности: Конституция Республики Беларусь, Уголовный Кодекс Республики Беларусь

1. [Средства защиты информации.](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1#p15)

I. **Формальные средства защиты** – выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека.

**Физические средства** - механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно от информационных систем, создавая различного рода препятствия на пути дестабилизирующих факторов (замок на двери, жалюзи, забор, экраны).

**Аппаратные средства** - механические, электрические, электромеханические, электронные, электронно-механические, оптические, лазерные, радиолокационные и тому подобные устройства, встраиваемые в информационных системах или сопрягаемые с ней специально для решения задач защиты информации.

**Программные средства** - пакеты программ, отдельные программы или их части, используемые для решения задач защиты информации. Программные средства не требуют специальной аппаратуры, однако они ведут к снижению производительности информационных систем, требуют выделения под их нужды определенного объема ресурсов и т.п.

К **специфическим средствам защиты информации** относятся криптографические методы. В информационных системах криптографические средства защиты информации могут использоваться как для защиты обрабатываемой информации в компонентах системы, так и для защиты информации, передаваемой по каналам связи. Само преобразование информации может осуществляться аппаратными или программными средствами, с помощью механических устройств, вручную и т.д.

II. **Неформальные средства защиты** – регламентируют деятельность человека.

**Законодательные средства** – законы и другие нормативно-правовые акты, с помощью которых регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Распространяются на всех субъектов информационных отношений.

**Организационные средства** - организационно-технические и организационно-правовые мероприятия, осуществляемые в течение всего жизненного цикла защищаемой информационной системы (строительство помещений, проектирование информационных систем, монтаж и наладка оборудования, испытания и эксплуатация информационных систем). Другими словами – это средства уровня организации, регламентирующие перечень лиц, оборудования, материалов и т.д., имеющих отношение к информационным системам, а также режимов их работы и использования. К организационным мерам также относят сертификацию информационных систем или их элементов, аттестацию объектов и субъектов на выполнение требований обеспечения безопасности и т.д.

**Морально-этические средства** - сложившиеся в обществе или в данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение приравнивается к несоблюдению правил поведения в обществе или коллективе, ведет к потере престижа и авторитета.

1. [Способы передачи конфиденциальной информации на расстоянии.](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1#p16)

Способов передачи конфиденциальной информации на расстоянии существует множество, среди которых можно выделить **три** основных направления.

1. Создать абсолютно надежный, недоступный для других канал связи между абонентами.

2. Использовать общедоступный канал связи, но скрыть сам факт передачи информации.

3. Использовать общедоступный канал связи, но передавать по нему нужную информацию в таком преобразованном виде, чтобы восстановить ее мог только адресат.

Проанализируем эти возможности.

1. С древних времен практиковалась охрана документа (носителя информации) физическими лицами, передача его специальным курьером (человеком (дипломатом) или животным (голубиная почта)) и т.д. Но, документ можно выкрасть, курьера можно перехватить, подкупить, в конце концов, убить. В настоящий момент для реализации данного механизма защиты используются современные телекоммуникационные каналы связи. Однако следует заметить, что данный подход требует значительных капитальных вложений. При современном уровне развития науки и техники сделать такой канал связи между удаленными абонентами для многократной передачи больших объемов информации практически нереально.

2. Разработкой средств и методов скрытия факта передачи сообщения занимается [стеганография](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema19). Первые следы стеганографических методов теряются в глубокой древности. Так, в трудах древнегреческого историка Геродота встречается описание двух методов сокрытия информации: на обритую голову раба записывалось необходимое сообщение, а когда его волосы отрастали, он отправлялся к адресату, который вновь брил его голову и считывал доставленное сообщение. Второй способ заключался в следующем: сообщение наносилось на деревянную дощечку, а потом она покрывалась воском, и, тем самым, не вызывала никаких подозрений. Потом воск соскабливался, и сообщение становилось видимым. В настоящий момент стеганографические методы в совокупности с криптографическими нашли широкое применение в целях сокрытия и передачи конфиденциальной информации.

3. Разработкой методов преобразования информации с целью ее защиты от несанкционированного прочтения занимается [криптография](https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema3#kriptografia).