безопасности информации при применении информационных технологий [Р 50.1.053-2005].

2. Постоянное наблюдение за процессом обеспечения безопасности информации в системе информационной с целью установить его соответствие требованиям безопасности информации [ГОСТ Р 50922-2006].

Мошенничество в сфере компьютерной информации

Хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [Уголовный кодекс РФ] (Глава 21, Статья 159.6).

Набор ключей конфиденциальный (*validator*)

Комплект, состоящий из ключа секретного схемы подписи цифровой, соответствующего ключа открытого и его сертификата ключа, используемый в системах-платежей электронных автономных с бумажниками электронными. Н. к. к. выдается специальным органом (центром выдачи н. к. к.), создаваемым для этих целей, вслепую так, что впоследствии центр выдачи н. к. к. не сможет идентифицировать клиента, которому был выдан данный н. к. к. Тем самым обеспечивается неотслеживаемость клиентов [Словарь крипт. терминов].

Набор тестов статистических (*battery of tests*)

В криптографии — совокупность статистических критериев (тестов), предназначенная для проверки соответствия анализируемой последовательности гипотезе о независимости и равновероятности ее элементов. Каждый тест состоит в вычислении по анализируемой последовательности некоторой статистики, имеющей известное распределение для последовательности случайной идеальной, и использовании критерия согласия. Стандартными н. т. с. являются набор тестов Д. Кнута, пакет *DIEHARD* (Дж. Марсальи), набор тестов *NIST* (Института стандартов США), пакет *TestUOl* (Л'Экуйера). В эти наборы входят тест автокорреляции, тест бита следующего, тест профиля сложности линейной, тест серий, тест универсальный Маурера, тест частотный и другие [Словарь крипт. терминов].

Наводки электромагнитные

Токи и напряжения в токопроводящих элементах, электрические

заряды или магнитные потоки, вызванные электромагнитным полем [ГОСТ Р 51624-2000].

Надежность (*reliability*)

Характеристика способности функционального узла, устройства, системы выполнять при определенных условиях требуемые функции в течение определенного периода времени. Показателями надежности являются вероятность безотказной работы, среднее время наработки на отказ, среднее время восстановления [Комов-09].

Надзор за соблюдением лицензиатами лицензионных требований и условий

Система мер, осуществляемых органами лицензирующими, государственными надзорными и контрольными органами в пределах их компетенции в целях обеспечения соблюдения лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий [N 158-ФЗ].

Нападающий (*attacker*)

Субъект, действия которого нарушают безопасность информации в рассматриваемой системе компьютерной.

Направления международного сотрудничества Российской Федерации в области обеспечения безопасности информационной основные

Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются:

- запрещение разработки, распространения и применения «информационного оружия»;
- обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;
- координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;
- предотвращение доступа несанкционированного к информации конфиденциальной в международных банковских сетях телекоммуникационных и системах информационного обеспечения мировой торговли, к информации международных правоохранительных

организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми [Доктрина ИБ].

Нарушение безопасности (системы информационной) (*security violation*)

Нарушение установленных правил управления доступом, приведшее к нарушению свойств конфиденциальности, целостности и доступности. Может быть, как преднамеренное в результате неправомерных действий злоумышленника, так и в результате сбоя в работе отдельных программ или технических компонентов системы.

Нарушение полномочий (*privilege violation*)

Попытка пользователя или программы выполнить неразрешенную операцию.

Нарушение системы безопасности (*security system violation*)

Успешное поражение средства управления безопасностью, которое завершается проникновением в систему [Комов-09].

Нарушение целостности информации (*information integrity violation*)

Утрата информации, при ее обработке техническими средствами, свойства целостности в результате ее несанкционированной модификации или несанкционированного уничтожения. Несанкционированная модификация информации может быть случайной (искажение) или умышленной (подделка). По отношению к целостности информации можно дифференцировать дополнительно следующие виды угроз: модификацию, искажение, подделку и уничтожение [Комов-09].

Нарушитель (*dishonest party*)

Участник протокола, нарушающий предписанные протоколом действия [Словарь крипт. терминов].

Син.: Участник нечестный, Нарушитель внутренний.

Нарушитель активный (*active adversary*)

Нарушитель, который недопустимым образом влияет на ход выполнения протокола криптографического. Как правило, полный анализ всех результатов однократного выполнения протокола криптографического позволяет обнаружить присутствие н. а. [Словарь крипт. терминов].

Нарушитель безопасности информационной

1. Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в системах информационных [Р 50.1.056-2005].

2. Физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение безопасности информационной организации [ГОСТ Р 53114-2008].

3. Субъект, реализующий угрозы безопасности информационной организации банковской системы Российской Федерации, нарушая предоставленные ему полномочия по доступу к активам организации банковской системы Российской Федерации или по распоряжению ими [СТО БР ИББС-1.0-2010].

Нарушитель в системе автоматизированной (информационной)

Субъект, имеющий доступ к работе со штатными средствами системы автоматизированной и средствами вычислительной техники как части системы автоматизированной [РД Концепция].

Нарушитель внешний (*outside adversary*)

См. Противник.

Нарушитель внутренний (*inside adversary*)

См. Нарушитель.

Нарушитель пассивный (*passive adversary, eavesdropper*)

Нарушитель, который ограничивается сбором и анализом информации о ходе выполнения протокола криптографического, но не вмешивается в него. Полный анализ результатов неоднократного выполнения криптографического протокола не позволяет обнаружить присутствие н. п. [Словарь крипт. терминов].

Нарушитель правил разграничения доступа (*security policy violator*)

Субъект доступа, осуществляющий несанкционированный доступ к информации [РД Защита от НСД], [РД АС].

Национальная безопасность Российской Федерации

Безопасность многонационального народа как носителя суверенитета и единственного источника власти, общества и государства [Концепция НБ РФ].

Национальные интересы России в информационной сфере

1. Соблюдение конституционных прав и свобод граждан в области

получения информации и пользования ею, развитие современных телекоммуникационных технологий, защита государственных ресурсов информационных от доступа несанкционированного [Концепция НБ ВС].

2. Выделяют четыре основные составляющие национальных интересов Российской Федерации в сфере информационной:

- соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;
- информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным ресурсам информационным;
- развитие современных технологий информационных, отечественной индустрии информации, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных ресурсов информационных. На этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности;
- защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности систем информационных и телекоммуникационных [Доктрина ИБ].

Национальные интересы Российской Федерации

Совокупность сбалансированных интересов личности, общества и государства в экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других сферах [Концепция НБ РФ].

Национальный библиотечно-информационный фонд Российской Федерации

Собрание всех видов обязательного экземпляра, комплектуемое на основе обязательного бесплатного экземпляра, распределяемое между книжными палатами, библиотеками, органами научно-технической информации, предназначенное для постоянного хранения и общественного использования [N 77-ФЗ].

Национальный центр безопасности компьютерной США (*National Computer Security Center (NCSC)*)

Организация, поддерживающая и стимулирующая распространение защищенных систем в учреждениях Федерального правительства. Является координирующим органом в области анализа и разработки систем с гарантированной защитой. Первичное название — Центр Компьютерной Безопасности министерства обороны США (*DoD Computer Security Center*) [Комов-09].

Невозможность отказа (*non-repudiation*)

1. Сервис, предназначенный для сбора, обработки и обоснования неопровержимой очевидности информации, касающейся предъявленного события или действия, с целью разрешения спора о том, что событие или действие имело место в реальности [ISO/IEC 10181-4].

2. Свойство протокола криптографического, состоящее в том, что его участники (все или некоторые) не могут отказаться от факта совершения определенных действий. Обеспечивается системой подписи цифровой [Словарь крипт. терминов].

3. Способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты [ИСО/МЭК 13888-1], [ГОСТ Р ИСО 7498-2-99].

Син.: Неотказуемость, Неотрекаемость.

Невозможность отказа от авторства (*non-repudiation of origin*)

Сервис, предназначенный для защиты от отрицания автором факта создания или отправления им сообщения [ISO/IEC 13888-1: 2009].

Неотказуемость

См. Невозможность отказа.

Неотрекаемость

См. Невозможность отказа.

Неотслеживаемость (*untracebility*)
Свойство, означающее невозможность получения противником и/или нарушителем сведений о действиях участников (протокола). Определяется для систем криптографических с большим количеством участников: систем платежей электронных, систем доступа к электронным информационным фондам и т. п. Родственные понятия — анонимность и несвязываемость [Словарь крипт. терминов].

Непрерывность защиты (*protection continuity*)
Принцип защиты, заключающийся в организации защиты объекта на всех стадиях его жизненного цикла: в период разработки, изготовления (строительства), испытаний, эксплуатации и утилизации.

Неприятие риска (*risk aversion*)
Отношение к риску, выражаемое в избегании риска [ISO GUIDE 73-2009].

Несвязываемость (*unlinkability*)
Свойство, родственное неотслеживаемости и означающее, что противник и/или нарушитель не только не может установить, кто именно выполнил данное конкретное действие, но даже выяснить, были ли разные действия выполнены одним и тем же участником [Словарь крипт. терминов].

Неформальный (*informal*)
Выраженный на естественном языке.

Норма эффективности защиты информации
Значение показателя эффективности защиты информации, установленное нормативными и правовыми документами [ГОСТ Р 50922-2006].

Носитель защищаемой информации
Физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин [ГОСТ Р 50922-2006].

Носитель информации (*data medium*)
Физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин [ГОСТ Р 50922-96].

Носитель сведений, составляющих тайну государственную

Материальные объекты, в том числе физические поля, в которых сведения, составляющие тайну государственную, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Примечание. Реквизиты носителей сведений, составляющих тайну государственную, включают следующие данные:

- о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;
- об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;
- о регистрационном номере;
- о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены [N 5485-1-ФЗ].

Нотаризация (*notarization*)

1. Регистрация данных доверенным третьим лицом, которое обеспечивает последующее подтверждение правильности их характеристик, таких как содержимое, отправитель, время и получатель [ОСТ 45.127-99].

2. Регистрация данных защищенной третьей стороной, что в дальнейшем позволяет обеспечить точность характеристик данных.

Примечание. К характеристикам данных, например, относятся: содержание, происхождение, время и способ доставки [Р 50.1.056-2005].

Син.: Заверение (подлинности).

Обезличивание персональных данных

Действия, в результате которых невозможно определить принадлежность данных персональных конкретному субъекту данных персональных [N 152-ФЗ].

Обеспечение безопасности информационной организации

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