Приволжский межрегиональный центр повышения квалификации и профессиональной переподготовки работников образования К(П)ФУ

Нормативное регулирование информационной безопасности в сети Интернет

Сафин Алексей Алексеевич,
кандидат педагогических наук

«За безопасность необходимо платить, а за ее отсутствие расплачиваться!»

Уинстон Черчилль

Понятие **«безопасность»** определено в Стратегии национальной безопасности Российской Федерации.

Понятие **«безопасность»** характеризуется как состояние защищенности личности, общества и государства от различных внешних и внутренних угроз и опасностей.

В Конституции Российской Федерации и действующем законодательстве предусматривается обеспечение **национальной безопасности** на всех ее уровнях (личном, общественном, государственном).

Предотвращение, преодоление и устранение возникающих в процессе жизнедеятельности угроз безопасности, а также выстраивание оптимальных приемлемых условий и создание новых возможностей и перспектив по обеспечению безопасности являются сутью и центральными **целями безопасности**.

Виды безопасности на всех ее уровнях (личном, общественном, государственном):

- информационная,
- экологическая,
- экономическая,
- энергетическая,
- социальная,
- профессиональная,
- психологическая,
- и другие виды безопасности

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, человеком и автоматом, автоматом и автоматом;

- сигналы в животном и растительном мире;

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

- и т.д.

В Доктрине информационной безопасности Российской Федерации под термином **информационная безопасность** понимается состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

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

Таким образом, концепция информационной безопасности, в общем случае, должна отвечать на три вопроса:

- Что защищать?

- От чего (кого) защищать?

- Как защищать?

Важнейшие компоненты информационной безопасности :

- доступность информации (своевременный беспрепятственный доступ правомочных субъектов к интересующей их информации);

- целостность информации (свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению);

- конфиденциальность информации (свойство информации быть известной и доступной только правомочным субъектам системы)

Основные объекты защиты при обеспечении информационной безопасности:

- все виды информационных ресурсов. Информационные ресурсы (документированная информация) - информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать;
- права граждан, юридических лиц и государства на получение, распространение и использование информации;
- система формирования, распространения и использования информации (информационные системы и технологии, библиотеки, архивы, персонал, нормативные документы и т.д.);
- система формирования общественного сознания (СМИ, социальные институты и т.д.).

Государственную тайну (владелец тайны – государство) защищают:

- межведомственная комиссия по защите государственной тайны;
- федеральные органы исполнительной власти, уполномоченные в области:
- в области обеспечения безопасности - Федеральная служба по техническому и экспортному контролю (ФСТЭК);
- обороны – Министерство обороны;
- внешней разведки – Федеральная служба безопасности (ФСБ обеспечивает, в т.ч. криптографическую защиту);
- противодействия техническим разведкам и технической защиты информации – ФСТЭК;
- другие органы.

Конфиденциальная информация:

- тайна следствия и судопроизводства;
- служебная тайна;
- профессиональная тайна;
- коммерческая тайна;
- сведения о сущности изобретения, полезной модели или промышленного образца по официальной публикации информации о них;
- персональные данные.

Персональные данные – это информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Права субъектов персональных данных:

- информационное самоопределение;
- доступ к своим персональным данным;
- внесение изменений в свои персональные данные;
- блокирование персональных данных;
- обжалование неправомерных действий в отношении персональных данных;
- возмещение ущерба.

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);
- «вредная» информация (информация, не подлежащая распространению как недостоверная, ложная, неприемлемая в обществе по нормам морали и т.п.).

Основными **носителями информации** являются:

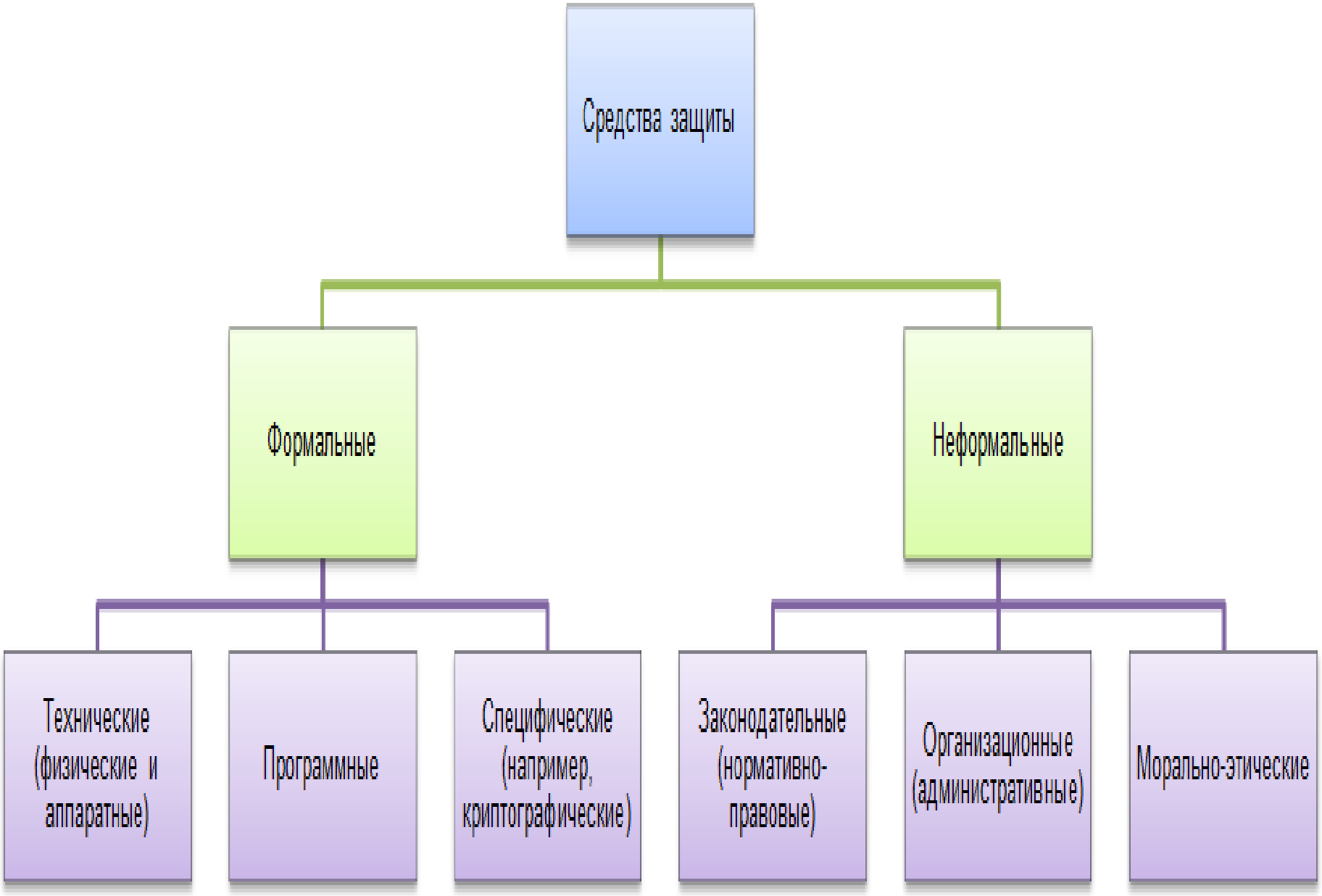
- открытая печать (газеты, журналы, отчеты, реклама и т.д.);

- люди;

- средства связи (радио, телевидение, телефон и т.д.);

- документы (официальные, деловые, личные и т.д.);

- электронные, магнитные и другие носители, пригодные для автоматической обработки данных.


Средства защиты
Формальные
Неформальные
Технические (физические и аппаратные)
Программные
Специфические (например, криптографические)
Законодательные (нормативно-правовые)
Организационные (административные)
Морально-этические

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

Включают:

-**физические средства** (замок на двери, жалюзи, забор, экраны и др);

-**аппаратные средства** (встраиваемые в информационные системы устройства защиты);

-**программные средства** (пакеты программ, используемые для решения задач защиты информации);

-**специфические средства** защиты (криптографические средства защиты информации: шифрование, кодирование и др.)

Неформальные средства защиты

(регламентируют деятельность человека):

- законодательные средства (законы и другие нормативно-правовые акты);

- **организационные средства** (организационно-технические и организационно-правовые мероприятия по защите информации);

- **морально-этические средства** (сложившиеся в обществе или в данном коллективе моральные нормы или этические правила работы с информацией)

Способы передачи конфиденциальной информации:

1. Создание надежного, недоступного для других канала связи между абонентами.

2. Использование общедоступного канала связи со скрытием самого факта передачи информации.

3. Использование общедоступных каналов связи, с передачей нужной информации в таком преобразованном виде, чтобы восстановить ее мог только адресат.

«Надежно защищен только выключенный компьютер!»

Евгений Касперский

Использованная литература

1.Федеральный закон Российской Федерации от 28 июля 2012 г. N 139-ФЗ "О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации»

2.Письмо МИНОБРНАУКИ РОССИИ от 28.04.2014 № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет»

3.Федеральный закон от 29 декабря 2010 года г. № 436-ФЗ (в ред. Федеральных законов от 28.07.2012 N 139-ФЗ, от 05.04.2013 N 50-ФЗ, от 29.06.2013 N 135-ФЗ,от 02.07.2013 N 185-ФЗ, от 14.10.2014) "О защите детей от информации, причиняющей вред их здоровью и развитию»

4.Письмо Минкомсвязи России от 14.08.2012 № 52-165/ВА "О применении норм Федерального закона от 29 декабря 2010 г. № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию»

Использованная литература

5.Письмо Минобрнауки России от 28.04.2014 № ДЛ-115/03 "О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет»

6.Приказ Минкомсвязи России от 16.06.2014 № 161"Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию" (Зарегистрировано в Минюсте России 12.08.2014 №33555)

7.Рекомендации по применению Федерального закона от 29 декабря 2010г. № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" в отношении печатной (книжной) продукции" (утв. Минкомсвязи России 22.01.2013 № АВ-П17-53)

8.Статья 13 Федерального закона от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» (пунктом 7 Положения о Министерстве юстиции Российской Федерации, утвержденного Указом Президента Российской Федерации от 13.10.2004 № 1313, на Минюст России возложены функции по ведению, опубликованию и размещению в сети Интернет федерального списка экстремистских материалов. http://www.minjust.ru/nko/fedspisok - Федеральный список экстремистских материалов