ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

ЛЕКЦИЯ 16. ТЕМА 1.16. БЕЗОПАСНОСТЬ В ЦИФРОВОЙ СРЕДЕ

1. Понятие цифровой среды и цифрового следа

Цифровая среда представляет собой совокупность информационных систем, сетей связи, сайтов в сети «Интернет», информационных технологий и субъектов, деятельность которых связана с формированием, обработкой и передачей информации в электронном виде. Данное понятие производно от определения информационной сферы, закреплённого в Доктрине информационной безопасности Российской Федерации, утверждённой Указом Президента РФ от 05.12.2016 № 646. Согласно этому документу, информационная сфера — это совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, а также совокупность механизмов регулирования соответствующих общественных отношений.

Базовым нормативным актом, определяющим ключевые термины в данной области, выступает Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Закон определяет информацию как сведения (сообщения, данные) независимо от формы их представления, а информационно-телекоммуникационную сеть — как технологическую систему, предназначённую для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Цифровой след — это информация о действиях пользователя в цифровой форме, а также данные о компьютерных или электронных устройствах, которые могут использоваться для выявления, раскрытия и расследования IT-правонарушений. Данное определение было официально утверждено Минцифры России в проекте доктрины по борьбе с IT-преступлениями в июле 2026 года. В этом же документе закреплено понятие цифровой гигиены — совокупности знаний, навыков и правил безопасного поведения граждан и организаций в цифровой среде, направленных на предупреждение IT-правонарушений.

Цифровой след формируется непрерывно: каждый запрос в поисковой системе, каждое сообщение в мессенджере, каждая транзакция через банковское приложение, каждый проход через систему контроля доступа с биометрической идентификацией оставляют цифровые записи. Эти записи могут быть использованы как для обеспечения безопасности (например, при расследовании преступлений), так и против интересов субъекта — при несанкционированном доступе, утечках или целенаправленном сборе данных.

2. Влияние цифровой среды на жизнь человека

Цифровая среда в современном её состоянии пронизывает все сферы жизнедеятельности: коммуникацию, трудовую деятельность, образование, финансы, здравоохранение, государственное управление. Согласно Доктрине информационной безопасности, информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства.

Положительное влияние цифровой среды включает обеспечение оперативного доступа к государственным и коммерческим сервисам, возможность дистанционного получения образования и медицинской помощи, повышение эффективности экономических процессов. Однако то же проникновение цифровых технологий порождает ряд проблем: размывание границ между приватной и публичной сферами, рост психоэмоциональной нагрузки, связанной с постоянным пребыванием в информационном потоке, и появление новых видов угроз, не имевших аналогов в доцифровую эпоху.

Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации, утверждённая распоряжением Правительства РФ от 22.12.2022 № 4088-р, фиксирует, что стремительное развитие информационных технологий затрагивает практически все сферы общественной жизни, и определяет культуру информационной безопасности как совокупность сформированных знаний, умений и навыков по вопросам информационной безопасности, обеспечивающую безопасное пребывание гражданина в информационном пространстве.

3. Приватность и персональные данные

Приватность в цифровой среде — это состояние защищённости личной информации субъекта от несанкционированного доступа, использования и распространения. Правовую основу защиты персональных данных в Российской Федерации составляет Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (действует в редакции от 26.07.2026). Целью данного закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Персональные данные в соответствии со статьёй 3 закона № 152-ФЗ определяются как любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу. Закон выделяет следующие категории:

• **Общедоступные персональные данные** — сведения, включённые в общедоступные источники с письменного согласия субъекта (статья 8);

• **Специальные категории персональных данных** — сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни (статья 10). Обработка таких данных по общему правилу не допускается;

• **Биометрические персональные данные** — сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность (статья 11). Обработка возможна только при наличии согласия в письменной форме.

Статья 7 закона № 152-ФЗ устанавливает принцип конфиденциальности: операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта, если иное не предусмотрено федеральным законом.

Важно отметить, что трансграничная передача персональных данных регулируется статьёй 12 закона и может быть запрещена или ограничена в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

4. Цифровая зависимость: признаки и последствия

Цифровая зависимость (цифровая аддикция) — это патологическая тяга к использованию цифровых устройств и онлайн-сервисов, при которой интернет-активность начинает превалировать над остальными жизненными потребностями и интересами. С 2022 года гаджетомания официально внесена в Международную классификацию болезней (МКБ-10). Одной из наиболее распространённых форм является номофобия (no mobile phone phobia) — страх остаться без доступа к мобильному устройству.

Согласно данным Мониторинга цифровой трансформации общества, проведённого Институтом статистических исследований и экономики знаний НИУ ВШЭ в 2026 году, признаки тяжёлой зависимости от интернета обнаружены у 13% опрошенных, ещё у 21% — умеренно выраженные симптомы. Среди молодёжи 18–24 лет доля лиц с тяжёлой формой зависимости достигает 22%.

В исследовании, проведённом сервисом SuperJob, 43% россиян признают у себя признаки цифровой зависимости. Среди респондентов до 24 лет этот показатель составляет 54%, среди лиц старше 45 лет — 35%.

Ключевые признаки сформировавшейся цифровой зависимости включают:

1. **Утрату контроля над временем** — 60% пользователей остаются онлайн дольше, чем планировали;
2. **Неспособность сократить время онлайн** — 18% респондентов регулярно пытаются, но не могут это сделать;
3. **Нарушение повседневного уклада** — 20% недосыпают из-за интернета, 22% предпочитают онлайн-общение реальным встречам;
4. **Синдром отмены** — раздражение, тревога или паника при попытке ограничить время использования устройства;
5. **Сужение интересов** — потеря интереса к прежним увлечениям, заменённым онлайн-активностью.

Нейробиологические последствия цифровой зависимости включают клиповое мышление (неспособность к длительной концентрации), нарушения сна (подавление выработки мелатонина синим светом экранов), тревожность и истощение дофаминовых рецепторов, снижение эмпатии при замене реального общения виртуальным.

5. Опасности и риски цифровой среды: источники и классификация

Опасности цифровой среды можно классифицировать по нескольким основаниям.

По характеру воздействия (в соответствии с ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»):

- **Несанкционированный доступ** — получение защищаемой информации заинтересованными субъектами с нарушением установленных прав или правил разграничения доступа;
- **Преднамеренное воздействие** — целенаправленное воздействие на защищаемую информацию, в том числе с применением электромагнитных или иных физических полей, в криминальных или террористических целях;
- **Непреднамеренное воздействие** — воздействие, вызванное ошибками пользователя, сбоем технических и программных средств, природными явлениями.

По источнику возникновения:

1. **Технические** — уязвимости программного обеспечения, сбои оборудования, перехват данных в открытых каналах связи;
2. **Социальные** — методы социальной инженерии, при которых злоумышленники манипулируют доверием пользователя для получения доступа к конфиденциальной информации;
3. **Правовые** — недостаточная регламентация отдельных аспектов обработки данных, пробелы в законодательстве;
4. **Психологические** — информационно-психологические угрозы, включая травлю в цифровом пространстве, пропаганду насилия, распространение недостоверной информации.

Доктрина информационной безопасности Российской Федерации определяет угрозу информационной безопасности как совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере. Стратегическими целями в области государственной и общественной безопасности названы защита суверенитета, поддержание политической и социальной стабильности, обеспечение основных прав и свобод человека, а также защита критической информационной инфраструктуры.

6. Кража персональных данных и паролей

Хищение персональных данных квалифицируется по нескольким статьям Уголовного кодекса Российской Федерации:

• **Статья 272 УК РФ** — неправомерный доступ к компьютерной информации, если это привело к уничтожению, блокированию, модификации или копированию данных;

• **Статья 272.1 УК РФ** — незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные. Часть 1 предусматривает штраф до 300 000 рублей или лишение свободы на срок до 4 лет. Часть 2 (в отношении данных несовершеннолетних, специальных категорий и биометрических данных) — штраф до 700 000 рублей или лишение свободы до 5 лет. Часть 6 устанавливает ответственность за создание информационных ресурсов, заведомо предназначенных для незаконного хранения и распространения похищенных персональных данных;

• **Статья 137 УК РФ** — нарушение неприкосновенности частной жизни, распространение сведений, составляющих личную или семейную тайну.

Административная ответственность за правонарушения в сфере обработки персональных данных предусмотрена статьёй 13.11 КоАП РФ.

Кража паролей осуществляется преимущественно через фишинг — массовые рассылки электронных писем и сообщений, имитирующих коммуникацию от доверенных организаций, с целью получения логинов, паролей, данных банковских карт. Также распространён вишинг (голосовой фишинг) — манипулирование телефонными сетями для получения личной и финансовой информации.

7. Мошенничество в цифровой среде и правила защиты

Мошенничество в цифровой среде охватывается несколькими статьями УК РФ:

• **Статья 159 УК РФ** — мошенничество, то есть хищение чужого имущества путём обмана или злоупотребления доверием. Максимальное наказание по части 4 — лишение свободы на срок до 10 лет;

• **Статья 159.3 УК РФ** — мошенничество с использованием электронных средств платежа;

• **Статья 159.6 УК РФ** — мошенничество в сфере компьютерной информации, то есть хищение путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи данных. Максимальное наказание по части 4 — лишение свободы на срок до 10 лет.

Основные схемы мошенничества в цифровой среде:

1. **Фишинг и вишинг** — получение учётных данных и кодов через поддельные сайты и телефонные звонки;
2. **SMS-мошенничество** — рассылка сообщений о блокировке счетов с требованием сообщить данные карты и коды;
3. **Социальная инженерия** — представление сотрудниками служб, предложения финансовых выигрышей, использование нейротехнологий для подделки голосов и видеосообщений от имени знакомых;
4. **Мошенничество с предоплатой** — размещение фиктивных объявлений о продаже товаров и услуг;
5. **Взлом аккаунтов** — несанкционированный доступ к учётным записям в социальных сетях с последующей рассылкой просьб о финансовой помощи от имени владельца аккаунта.

Правила защиты от мошенников, сформулированные Минцифры России в рекомендациях по цифровой гигиене (письмо от 17.09.2024 № П25-305029) и поддержанные Концепцией формирования и развития культуры информационной безопасности:

• Завершать разговор при подозрении на мошенничество и перезванивать в организацию по официальному номеру;

• Не сообщать логины, пароли и коды из SMS ни при каких обстоятельствах;

• Читать назначение SMS-кодов и не делиться ответами на контрольные вопросы;

• Следить за актуальностью номера телефона, привязанного к аккаунту;

• Использовать сложные пароли длиной не менее 12 символов с комбинацией букв, цифр и специальных знаков;

• Не использовать один и тот же пароль для разных учётных записей;

• Обновлять пароли не реже одного раза в полгода;

• Подключить двухфакторную аутентификацию;

• Проверять адрес открываемых страниц, убеждаясь, что сайт является официальным ресурсом.

8. Правила безопасного поведения в цифровой среде

Концепция формирования и развития культуры информационной безопасности граждан, утверждённая распоряжением Правительства РФ от 22.12.2022 № 4088-р, определяет, что культура информационной безопасности затрагивает как профессиональную, так и бытовую деятельность граждан. Стратегической целью государственной политики в этой области является формирование у граждан навыков противодействия угрозам информационной безопасности, в том числе информационно-психологическим.

Базовые правила безопасного поведения в цифровой среде:

1. **Осознанное формирование цифрового следа** — понимание того, что каждое действие в сети оставляет запись, которая может быть использована для идентификации, профилирования или атаки;
2. **Минимизация раскрываемой информации** — предоставление только тех данных, которые необходимы для конкретной транзакции или сервиса;
3. **Проверка источников информации** — критическая оценка достоверности контента, особенно в случаях, когда от него зависит принятие финансовых или юридических решений;
4. **Регулярный аудит цифровых аккаунтов** — удаление неиспользуемых учётных записей, проверка разрешений, предоставленных приложениям;
5. **Сегментирование данных** — разделение личной, рабочей и публичной информации, использование разных учётных записей и устройств для разных задач;
6. **Контроль экранного времени** — ограничение времени пребывания в цифровой среде для предотвращения формирования зависимости и снижения когнитивных функций.

9. Правила безопасного использования устройств и программ

Минцифры России в рекомендациях по кибергигиене (письмо от 17.09.2024 № П25-305029) сформулировало ряд правил, применимых к использованию устройств и программного обеспечения:

Защита от вредоносного ПО и несанкционированного доступа:

• Не подключать к компьютерам неизвестные внешние носители информации (USB-накопители, диски);

• Не открывать вложения с подозрительными расширениями (.zip, .js, .exe);

• Не открывать файлы, требующие включения поддержки макросов, без уверенности в их источнике;

• Не открывать письма и чаты от незнакомых отправителей;

• С осторожностью относиться к письмам с призывами к действиям или темами о финансах и угрозах.

Обновление и техническое обслуживание:

• Своевременно устанавливать обновления операционной системы и прикладного программного обеспечения — новые версии закрывают выявленные уязвимости и защищают от известных киберугроз;

• Использовать антивирусное программное обеспечение и регулярно проводить проверку устройств;

• Создавать резервные копии важных данных — игнорирование резервного копирования становится угрозой потери данных при атаке или сбое.

Защита учётных записей:

• Использовать сложные пароли (не менее 12 символов, включающие буквы разных регистров, цифры и специальные знаки);

• Не использовать одинаковые пароли для разных учётных записей;

• Регулярно (не реже раза в полгода) обновлять пароли, в том числе от учётных записей уволенных или переведённых сотрудников;

• Включать двухфакторную аутентификацию во всех сервисах, где она доступна.

Цифровая гигиена как системная практика:

• Не открывать социальные сети первые 30 минут после пробуждения;

• Отключать всплывающие уведомления во время работы над конкретной задачей;

• Не использовать дисплей за один-два часа до сна, ограничивать яркость и синий свет;

• Периодически проводить «цифровой детокс» — сознательный отказ от использования цифровых устройств на определённое время.

10. Заключение

Безопасность в цифровой среде представляет собой комплексную задачу, решение которой требует согласованных действий на трёх уровнях: нормативно-правовом, организационно-техническом и индивидуальном. Нормативно-правовой уровень обеспечивается системой федеральных законов (№ 149-ФЗ, № 152-ФЗ), Уголовного кодекса РФ, государственных стандартов (ГОСТ Р 50922-2006) и стратегических документов (Доктрина информационной безопасности, Концепция формирования культуры информационной безопасности). Организационно-технический уровень реализуется через применение средств защиты информации, систем аутентификации и контроля доступа, антивирусного ПО. Индивидуальный уровень — это культура информационной безопасности гражданина, совокупность его знаний, умений и навыков, обеспечивающая безопасное пребывание в информационном пространстве.

Ключевой вывод состоит в том, что технологические средства защиты, сколь бы совершенными они ни были, не заменяют осознанного и ответственного поведения пользователя. Цифровой след, оставляемый каждым действием в сети, является одновременно инструментом безопасности и источником уязвимости. Понимание этого дуализма и формирование навыков цифровой гигиены составляют фундамент личной безопасности в цифровой среде.