ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НИЖЕГОРОДСКАЯ АКАДЕМИЯ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ

РОССИЙСКОЙ ФЕДЕРАЦИИ»

Кафедра математики, информатики и информационных технологий

|  |  |  |
| --- | --- | --- |
|  |  | УТВЕРЖДАЮ  Начальник кафедры математики, информатики и информационных технологий НА МВД России  полковник полиции  С.Н. Сухов  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |

**Конспект**

**занятия лекционного типа**

**по теме №1 «Основные понятия информационной безопасности органов внутренних дел»**

дисциплины «Основы информационной безопасности в органах внутренних дел»

по специальности 40.05.02 Правоохранительная деятельность,

специализации – оперативно-розыскная деятельность

(узкой специализации – деятельность оперуполномоченного уголовного розыска)

(для набора 2019 года заочной формы обучения)

**Разработчик:**

Материалы, содержащиеся в конспекте занятия лекционного типа, вычитаны, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, доступ к которым и распространение ограничены.

Профессор преподаватель кафедры математики,

информатики и информационных технологий

Нижегородской академии МВД России

д.ю.н., профессор В.И. Шаров

Обсужден и одобрен на заседании кафедры математики, информатики и информационных технологий (протокол №22 от 20.03.2020 г.).

Нижний Новгород

2020

**1. Тема занятия, количество часов, отводимых на данное занятие.**

Основные понятия информационной безопасности органов внутренних дел (2 часа)

**2. Цель и задачи занятия.**

**Цель:** рассмотреть основы информационной безопасности и защиты информации и особенности обеспечения информационной безопасности в органах внутренних дел.

**Задачи занятия:**

1. Рассмотреть основные понятия информационной безопасности и защиты информации.
2. Рассмотреть меры защиты информации, направленные на обеспечение информационной безопасности.
3. Дать характеристику угроз информационной безопасности.
4. Рассмотреть особенности обеспечения информационной безопасности в органах внутренних дел.

**3. Учебные вопросы.**

1. Основные понятия информационной безопасности и защиты информации.

2. Обеспечение информационной безопасности. Защита информации.

3. Угрозы безопасности информации.

4. Обеспечение информационной безопасности в органах внутренних дел.

**4. Рекомендуемая литература по данному занятию.**

1. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие / Ю. Н. Загинайлов. – М. : Берлин : Директ-Медиа, 2015. – 253 с.– URL: http://biblioclub.ru/index.php?page=book&id=276557.
2. Крыгин, С. В. Основы информационной безопасности и защита информации в ОВД : учеб. практ. пособие / С. В. Крыгин, С. Н. Сухов, Т. Е. Чикина ; МВД России, НА. – Н. Новгород : НА МВД России, 2018. – 128 с. – То же [Электронный ресурс]. – Режим доступа: https://namvd.bibliotech.ru/Reader/Book/2018071116344792879200002803.
3. Шаров, В. И. Основы информационной безопасности в ОВД : учеб. пособие / В. И. Шаров, С. В. Крыгин, Н. Г. Лабутин; МВД России, НА. – Н. Новгород : НА МВД России, 2016. – 126 с. – То же [Электронный ресурс]. – Режим доступа: https://namvd.bibliotech.ru/Reader/Book/2017042716204648608200008495.

**5. Краткое описание учебных вопросов.**

**1.** **Основные понятия информационной безопасности и защиты информации**

Информационная безопасность довольно новое понятие, получившее свое развитие в условиях развития современных компьютерных и телекоммуникационных технологий. Увеличение объемов передаваемой и обрабатываемой информации, увеличение ее значимости в современном мире привело к тому, что обеспечение информационной безопасности становится все более актуальной и важной задачей. Сегодня информационная безопасность представляется основой функционирования любой организации, а потеря информационных ресурсов ставит под вопрос само ее существование.

Определяющую роль информационная безопасность играет и в системе национальной безопасности страны, поскольку государственная информационная политика тесно взаимодействует с государственной политикой обеспечения национальной безопасности страны, где информационная безопасность выступает важным связующим звеном всех основных компонентов государственной политики в единое целое.

*Под информационной безопасностью* сегодня понимается такое состояние информации, которое бы препятствовало воздействию на нее с целью нанесения ущерба участникам информационных правоотношений, защищенность информации от внешних воздействий (попыток неправомерного копирования, распространения, модификации либо уничтожения). Информационная безопасность представляется состоянием системы, рассматриваемой с двух сторон: с одной стороны, как способность противостоять дестабилизирующему воздействию внешних и внутренних факторов, а с другой, чтобы само функционирование этой системы не создавало угроз для нее самой и внешней среды.

В официальных документах *информационная безопасность* Российской Федерации определяется как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором *обеспечиваются* реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Определенный данными понятиями *подход к информационной безопасности*, фактически, как системы превентивных мер, обеспечивающих защищенность информационных ресурсов, тем не менее исходит из создания мер противодействия конкретным угрозам информационной безопасности. Тем самым формируется методологический подход к проблемам обеспечения информационной безопасности, реализуемый посредством определения ключевых интересов субъекта в информационной сфере – вскрытие угроз информационной безопасности – выявления источника угроз – определения мер противодействия и нейтрализации этих угроз.

Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Это в первую очередь зависит от важности информации, имеющейся на защищаемом объекте. Понятно, что для защиты государственной тайны создается максимально закрытая система информационной безопасности, исключающая любой доступ к защищаемой информации, в других случаях безопасность информации ограничивается лишь физической сохранностью информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства в информационной сфере. Этим требованиям должны удовлетворять все методы и способы защиты, используемые при создании и эксплуатации государственных информационных систем в целях защиты информации.

В области информационной безопасности создана достаточно обширная нормативно-правовая база.

Президентом РФ от 5 декабря 2016 г. № 646 утверждена Доктрина информационной безопасности Российской Федерации. Она представляет собой систему официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере. Это документ стратегического планирования в сфере обеспечения национальной безопасности РФ. Она является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

**2.** **Обеспечение информационной безопасности. Защита информации**

Информационная безопасность обеспечивается путем применения мер и средств защиты информации. Средства обеспечения информационной безопасности разнообразны, они включают правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности. *Защиту информации можно определить* как комплекс мероприятий, осуществляемых в рамках защиты информации и направленных на обеспечение информационной безопасности.

В методических документах защита информации в информационных системах определена примерно также. Приводится, что меры *защиты информации направлены* на обеспечение:

* целостности информации (исключение неправомерного уничтожения или модифицирования информации);
* конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации);
* доступности информации (исключение неправомерного блокирования информации).

Среди *защитных мер чаще* всего называют правовые, организационные и технические меры, которые направлены на решение трех ключевых задач (направлений) информационной безопасности: обеспечение конфиденциальности, целостности и доступности информации. Однако вполне понятно, что в рамках указных направлений и мер возможно многообразие средств и методов по защите информации. Учитывая, что меры по защите информации направлены на противодействию угрозам информационной безопасности, то множество дес­табилизирующих факторов, возможных способов воздействия и порождающих их причин еще в большей степени расширяют систему противостоящих им средств и методов по защите информации.

Информационная безопасность обеспечивается комбинацией различных защитных мер для обеспечения требуемого уровня защиты. Например, средства контроля доступа к информационным системам, должны подкрепляться заданным порядком действий персонала и физической защитой помещений.

*Правовые меры* защиты направлены на решение целого ряда вопросов, требующих нормативно-правового регулирования. Они формируются из действующих законов, указов Президента РФ и других нормативных актов, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и выступая сдерживающим фактором для потенциальных нарушителей.

Законодательные акты, регулирующие общие положения по информационной безопасности и защиты информации. В первую очередь, это законы:

* «Об информации, информационных технологиях и о защите информации» от 27.06.2006 г. № 149-ФЗ.
* «Об электронной подписи» от 06.04.2011 г. № 63-ФЗ.

Любая правовая регламентация должна дополняться мерами ответственности за совершение противоправных действий (правонарушений или преступлений). В Российском законодательстве предусматривается как уголовная, так и административная ответственность за противоправные деяния в области информации и информатизации, сведенные в главу 28 УК РФ и главу 13 Кодекса об административных правонарушениях.

Преступления в сфере компьютерной информации, которым посвящена глава 28 УК РФ, содержат три состава.

а) Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (ст. 272).

б) Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (ст. 273).

в) Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб (ст. 274).

Интересен новый состав, изложенный в ст. 159.6. Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации.

Кодекс об административных правонарушениях содержит специальную главу 13 «Административные правонарушения в области связи и информации».

Статьи 13.12-13.13 формулируют составы правонарушений в области защиты информации (нарушение правил защиты информации и незаконная деятельность в области защиты информации). Статья 13.11 устанавливает ответственность за нарушение порядка сбора, хранения, использования или распространения информации о гражданах, 13.14 – разглашение информации ограниченного доступа.

*Организационные (административные) меры* защиты направлены на решение многочисленных вопросов регламентации взаимодействие работников с техническими средствами и между собой, процессов функционирования системы обработки данных и использование ее ресурсов с тем, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. Организационные меры, предпринимаемые в целях защиты информации, достаточно обширны. Они включают:

* мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;
* мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);
* мероприятия с персоналом, его подбор и расстановку, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
* организацию охраны и надежного пропускного режима, исключающего возможность тайного проникновения на территорию и в помещения посторонних лиц и одновременно обеспечение удобства контроля прохода и перемещения сотрудников и посетителей;
* распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);
* организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;
* контроль и соблюдение временного режима труда и пребывания на территории персонала, организацию явного и скрытого контроля за работой пользователей;
* организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей;
* мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения и т.п.

*Физические меры* обеспечения безопасности определяют защиту от воздействия окружающей среды, создание препятствий на пути проникновения нарушителей на объект информатизации. Физические средства контроля безопасности включают прочность внутренних стен строения, дверные замки с кодовым набором, противопожарные системы и охрану. Физические средства, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации, осуществляют защиту персонала, материальных средств, финансов и информации от противоправных воздействий.

Основными направлениями физической защиты выступают следующие:

* физическое управление доступом;
* противопожарные меры;
* защита поддерживающей инфраструктуры;
* защита мобильных систем.

*Технические меры защиты* основаны на использовании специальных электронных устройств, которые предназначены для защиты каналов передачи информации, предотвращения утечки информации, а также поиск и обнаружение устройств снятия информации, установленных злоумышленником. Техническая защита – это совокупность специальных технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации. К техническим средствам защиты информации относятся самые различные по принципу действия, устройству и возможностям технические конструкции, обеспечивающие пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации.

*Программно-аппаратные меры защиты* – специальные пакеты программ или от­дельные программы, различные электронные устройства, включаемые в состав программного обеспечения ав­томатизированных систем с целью решении задач защиты информации. Это могут быть различные программы и аппаратно-программные комплексы по криптографическому преобра­зованию данных, контролю доступа, защиты от вирусов, и др.

Основой программных и одновременно с ними технических мер защиты являются следующие механизмы безопасности:

* идентификация и аутентификация пользователей;
* управление доступом;
* протоколирование и аудит;
* криптография;
* экранирование;
* обеспечение высокой доступности и т.д.

Все меры защиты информации взаимосвязаны между собой, дополняют друг друга, образуя комплексную защиту объекта.

**3.** **Угрозы безопасности информации**

Под угрозой безопасности информации понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Угрозы воздействия на информацию можно разделить на два типа: случайные и преднамеренные.

Под случайной угрозой понимают непреднамеренное изменение информации в процессе ввода, хранения, обработки или передачи. Случайные воздействия могут быть аппаратными и программными. В результате случайных воздействий на аппаратном уровне происходит физическое изменение сигналов либо носителей информации. *Причины случайных воздействий:*

отказы и сбои аппаратуры;

воздействия факторов внешней среды;

схемные и системно-механические ошибки разработчиков аппаратуры;

структурные, алгоритмические ошибки разработчиков программного обеспечения;

ошибки человека-оператора.

Преднамеренные угрозы связаны с различными действиями человека, которые в отличие от случайных преследуют цель нанесения ущерба управляемой системе или пользователям.

Умышленные угрозы подразделяются также на внутренние (возникающие внутри управляемой организации) и внешние.

Внутренние угрозы исходят от сотрудников организации, внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями).

*Основные угрозы безопасности информации*

несанкционированный доступ к информации (НСД);

утечка конфиденциальной информации;

ошибочное использование информационных ресурсов и т.д.

Несанкционированный доступ — это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.

Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны (утечка информации).

Поскольку несанкционированный доступ к информации реализуется только с использованием штатных аппаратных и программных средств, то он считается возможным в следующих случаях:

• отсутствует система разграничения доступа;

• непосредственное обращение к объектам доступа;

• создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

• сбой или отказ в информационной системе;

• ошибочные действия пользователей или обслуживающего персонала информационной системы;

• ошибки в системе разграничения доступа;

• фальсификация полномочий.

Если система разграничения доступа отсутствует, то злоумышленник, имеющий навыки работы в информационной системе, может получить без ограничений доступ к любой информации. В результате сбоев или отказов средств системы, а также ошибочных действий обслуживающего персонала и пользователей возможны состояния системы, при которых упрощается НСД. Злоумышленник может выявить ошибки в системе разграничения доступом и использовать их для НСД. Фальсификация полномочий является одним из наиболее вероятных каналов НСД.

**4.** **Обеспечение информационной безопасности в органах внутренних дел**

В Министерстве внутренних дел Российской Федерации эффективному развитию информационных технологий и их внедрению в деятельность органов внутренних дел также уделено значительное внимание.

Для решения стоящих перед органами внутренних дел задач реализуется комплекс мер, направленных на совершенствование информационного обеспечения ОВД на основе оснащения их современными техническими комплексами, внедрения в практическую деятельность новых и перспективных информационных технологий.

*Информационная безопасность ОВД*понимается состояние защищенности информации, информационных ресурсов и информационных систем ОВД, при котором обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, подделки, копирования, блокирования.

В целях создания концептуального базиса, определяющего политику обеспечения информационной безопасности в системе министерства, Департаментом ИТСЗИ во взаимодействии с государственными регуляторами в данной сфере проводится работа по актуализации принимаемых мер обеспечения информационной безопасности, основными из которых являются:

* организация комплекса мероприятий по защите от компьютерных атак на критически важные сегменты информационной инфраструктуры МВД России;
* разработка комплекса мероприятий по обеспечению информационной безопасности и защиты данных информационных систем МВД России с учетом «облачной архитектуры»;
* создание эффективных механизмов защиты от несанкционированного доступа при создании полномасштабной системы доступа различных категорий пользователей системы МВД России к информационным активам;
* выработка организационно-правовых решений по регистрации и внесению в единый реестр подразделений МВД России в качестве операторов обработки персональных данных.

Отдельно следует отметить новую для МВД России работу по защите персональных денных, опирающуюся на одноименный Федеральный закон. Для этого Министерством внутренних дел Российской Федерации разработаны:

* Методические рекомендации по обеспечению безопасности персональных данных при их обработке в автоматизированных информационных системах МВД России.
* Приказ МВД России от 6 июля 2012 г. №678 «Об утверждении инструкции по защите персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации».

Настоящая Инструкция определяет порядок выполнения мероприятий по защите персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации, устанавливает меры по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных, а также определяет обязанности должностных лиц.

Министерство внутренних дел Российской Федерации является оператором, организующим и (или) осуществляющим обработку ПДн, а также определяющим цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

В связи с этим Инструкция по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации, разработана в соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", иными нормативными правовыми актами Российской Федерации, регламентирующими порядок обработки персональных данных.

Методы и способы защиты информации, содержащейся в государственных информационных системах, определяются в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17

* Комплекс мер по обеспечению информационной безопасности и защиты данных информационных систем МВД России с учетом реализации «облачной архитектуры», введенный приказом МВД России от 16 января 2012 года №25.
* Приказ МВД России от 29 декабря 2016 г. №925 «О некоторых вопросах обработки персональных данных в МВД России», который утверждает Перечень персональных данных, обрабатываемых в МВД РФ.
* Приказ МВД России от 21.12.2017 № 949  
  "О некоторых мерах, направленных на обеспечение выполнения МВД России обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных», утверждающий «Правила обработки персональных данных в системе МВД России».

Особую значимость для Министерства имеет реализация первоочередных задач государственной политики в области межведомственного взаимодействия, направленных на модернизацию государственного управления и повышение уровня оказываемых Министерством госуслуг в условиях развитого информационного общества.

Комплекс ресурсных мероприятий включает в себя внедрение в деятельность органов внутренних дел современных технических средств защиты информации, средств криптографической защиты информации (шифровальной техники), включая работающее совместно с ними оконечное оборудование. Внедряется также специальная и контрольно-измерительная аппаратура, средства вычислительной и организационной техники в защищенном исполнении, системное, прикладное и специальное программное обеспечения к ним, а также мобильные устройства удаленного доступа к информационным базам данных.

Инфраструктура обеспечения информационной безопасности в системе МВД России продолжает развиваться. Так, в настоящее время созданы и функционируют целый ряд ведомственных органов по аттестации объектов информатизации, аккредитованных ФСТЭК России, оснащенных современным контрольно-измерительным и поисковым оборудованием. По результатам проведенных мероприятий по расширению функциональных возможностей единой ведомственной сети шифровальной связи МВД России, порядка 100 объектов на федеральном, межрегиональном (окружном) и региональном уровнях территориальных органов МВД России и более 350 ОВД на районном уровне обеспечены возможностью использования современной IP-шифровальной связи.

**6. Вопросы для самоконтроля.**

1. Дать определение информационной безопасности и защиты информации.

2. Дать характеристику концептуальных правовых актов в области информационной безопасности.

3. Виды мер обеспечения информационной безопасности.

4. Правовые меры защиты информации.

5. Организационные (административные) меры защиты информации.

6. Физические меры защиты информации.

7. Технические меры защиты информации.

8. Программно-аппаратные меры защиты информации.

9. Уголовная и административная ответственность за совершение информационных и компьютерных преступлений и правонарушений.

10. Понятие угрозы информационной безопасности, типы угроз информационной безопасности, несанкционированный доступ к информации.

11. Каналы утечки информации, причины и условия утечки информации.

12. Меры и мероприятия по защите информации.

13. Технические средства защиты информации.

14. Специфические методы обеспечения информационной безопасности в правоохранительной сфере, принципы и задачи обеспечения ИБ в ОВД.