Лекция 1/2
Основы обеспечения информационной безопасности в ОВД

Учебные вопросы:

1. Основные термины и определения информационной безопасности.
2. Основные принципы и условия обеспечения информационной безопасности.
3. Понятие политики безопасности.

Вопрос 1.
ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

ГОСТ Р 50922-2006

Национальный стандарт РФ.

«Защита информации. Основные термины и определения»

Защита информации.

Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Система защиты информации.

Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Политика безопасности (информации в организации).

Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Безопасность информации [данных].

Состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

К видам защиты информации относятся:

Физическая защита информации.
Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Правовая защита информации.
Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Техническая защита информации.

ТЗИ: Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Криптографическая защита информации.

Защита информации с помощью ее криптографического преобразования.

Способ защиты информации.

Порядок и правила применения определенных принципов и средств защиты информации.

К способам защиты информации будут относиться:

Защита информации от утечки.

Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

Примечание - Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации от несанкционированного воздействия.

ЗИ от НСВ: Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия.

Защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения.
Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа. ЗИ от НСД: Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Защита информации от преднамеренного воздействия.

ЗИ от ПДВ: Защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

Защита информации от [иностранной] разведки.

Защита информации, направленная на предотвращение получения защищаемой информации [иностранной] разведкой.

Объект защиты информации.

Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

К объектам защиты информации будут относиться:

Защищаемая информация.

Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Примечание

Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

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.
Защищаемый объект информатизации.
Объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.
Защищаемая информационная система.
Информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности.

Угроза (безопасности информации). Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

К угрозам безопасности информации будут относиться

Фактор, воздействующий на защищаемую информацию.
Явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.
Источник угрозы безопасности информации.
Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.
Уязвимость (информационной системы); *брешь*.
Свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

К способам оценки соответствия требованиям по защите информации относятся:

Лицензирование в области защиты информации.
Деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ.

Сертификация на соответствие требованиям по безопасности информации.
Форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

Вопрос 2
Основные принципы и условия обеспечения информационной безопасности

В самом общем смысле **информационная безопасность** – такое состояние информации и среды, которое исключает вред собственнику или владельцу этой информации.

стандартная модель безопасности, включающей три категории:

- конфиденциальность;
- целостность;
- доступность.

Модель безопасности

- **Конфиденциальность** – это доступность информации только определенному кругу лиц.
- **Целостность** – свойство сохранности информация в определенном необходимом виде.
- **Доступность** – возможность использования информации собственником при необходимости.

Цели и задачи системы информационной безопасности

Целью защиты информации является сведение к минимуму потерь, вызванных нарушением целостности данных, их конфиденциальности или недоступности информации для потребителей.

задачами системы ИБ являются:

1. своевременное выявление и устранение угроз безопасности ресурсам, причин и условий, способствующих финансовому, материальному и моральному ущербу;
2. создание механизма и условий оперативного реагирования на угрозы безопасности;
3. эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
4. создание условий для минимизации и локализации возможного ущерба, ослабления негативного влияния последствий.

Принципы системы ИБ являются

1. принцип непрерывного совершенствования системы информационной безопасности.
2. принцип комплексного использования всех доступных средств защиты

условиями обеспечения безопасности

1. законность,
2. достаточность,
3. соблюдение баланса интересов личности и организации,
4. профессионализм представителей службы безопасности,
5. подготовка пользователей и соблюдение ими всех установленных правил сохранения конфиденциальности,
6. взаимная ответственность персонала и руководства,
7. взаимодействие с государственными правоохранительными органами.

Требования к защите информации

1. централизованной;
2. плановой;
3. конкретной и целенаправленной;
4. активной;
5. экономически эффективной;
6. нестандартной
7. открытой
8. надежной и универсальной

Вопрос 3
Понятие политики безопасности

Политика безопасности организации (англ. *organizational security policies*) – совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которые регулируют управление, защиту и распределение ценной информации.

Цель планирования:

- координация деятельности соответствующих подразделений по обеспечению информационной безопасности;
- наилучшее использование всех выделенных ресурсов;
- предотвращение ошибочных действий, могущих привести к снижению возможности достижения цели.

Различают *два вида планирования*: стратегическое или перспективное и тактическое или текущее.

- **Стратегическое планирование** заключается в определении (без детальной проработки) средств и способов достижения конечных целей, в том числе необходимых ресурсов, последовательности и процедуры их использования.

- **Тактическое планирование** заключается в определении промежуточных целей на пути достижения главных. При этом детально прорабатываются средства и способы решения задач, использования ресурсов, необходимые процедуры и технологии.

Планирование включает в себя определение, разработку или выбор:

- конечных и промежуточных целей и обоснование задач, решение которых необходимо для их достижения;
- требований к системе защиты информации;
- средств и способов функциональной схемы защиты информации с учетом стоимости и привлечения других ресурсов;
- совокупности мероприятий защиты, проводимых в различные периоды времени;
- порядка ввода в действие средств защиты;
- ответственности персонала;
- порядка пересмотра плана и модернизации системы защиты;
- совокупности документов, регламентирующих деятельность по защите информации.

Политика безопасности ***должна гарантировать***, что для каждого вида проблем существует ***ответственный исполнитель***. В связи с этим ключевым элементом политики безопасности является доведение до каждого сотрудника его обязанностей по поддержанию режима безопасности.

Нужно уметь четко ответить на следующие вопросы:

- Сколько компьютеров установлено в организации? Сколько их на рабочих местах, сколько в ремонте, сколько в резерве.
- Можно ли узнать каждый компьютер «в лицо»?
- Можно ли обнаружить «маскарад» оборудования, когда какой-нибудь компьютер или его часть, или программное обеспечение подменены?
- Какие задачи и с какой целью решаются на каждом компьютере?
- Каков порядок ремонта и технической профилактики компьютеров?
- Как проверяется оборудование, возвращаемое из ремонта, перед установкой на рабочее место?
- Как производится изъятие и передача компьютеров в подразделения и каков порядок приема в работу нового оборудования и т.д.

Комплекс мероприятий, необходимых для реализации защиты информации на объекте по времени проведения

По времени проведения:

- разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия;
- периодически проводимые (через определенное время) мероприятия;
- мероприятия, проводимые при осуществлении или возникновении определенных условий или изменений в самой защищаемой системе или среде (по необходимости);
- постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия.

Разовые мероприятия:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов;
- разработка и утверждение функциональных обязанностей должностных лиц службы компьютерной безопасности;
- оформление юридических документов (в форме договоров, приказов и распоряжений руководства организации) по вопросам регламентации отношений с пользователями (клиентами), работающими в автоматизированной системе;
- определение порядка назначения, изменения, утверждения и предоставления конкретным должностным лицам необходимых полномочий по доступу к ресурсам системы;
- разработка правил управления доступом к ресурсам , оценка возможного ущерба, вызванного нарушением безопасности информации);
- организация пропускного режима;
- организация учета, хранения, использования и уничтожения документов и носителей с закрытой информацией;
- определение порядка проектирования, разработки, отладки, модификации, приобретения, исследования, приема в эксплуатацию, хранения и контроля целостности программных продуктов;
- создание отделов (служб) компьютерной безопасности;
- определение перечня регулярно проводимых мероприятий и оперативных действий персонала по обеспечению непрерывной работы и восстановлению вычислительного процесса в критических ситуациях.

Периодически проводимые мероприятия:

- Распределение и смена реквизитов разграничения доступа (паролей, ключей шифрования и т. п.).
- Анализ системных журналов и принятие мер по обнаруженным нарушениям правил работы.
- Мероприятия по пересмотру правил разграничения доступа пользователей к информации в организации.
- Осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты (периодически с привлечением сторонних специалистов.
- Мероприятия по пересмотру состава и построения системы защиты.

Мероприятия, проводимые по необходимости:

- мероприятия, осуществляемые при кадровых изменениях в составе персонала системы;
- мероприятия, осуществляемые при ремонте и модификациях оборудования и программного обеспечения;
- мероприятия по подбору и расстановке кадров (проверка принимаемых на работу, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно нарушать свои обязанности и т. д.).

Постоянно проводимые мероприятия:

- противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности техники и носителей информации и т. п.;
- явный и скрытый контроль за работой персонала системы;
- контроль за применением мер защиты.

Пересмотр **«Плана защиты»** рекомендуется производить ***раз в год.*** Кроме того, существует ряд случаев, требующих внеочередного пересмотра. К их числу относятся изменения следующих компонентов объекта:

- **Люди.** Пересмотр может быть вызван кадровыми изменениями, связанными с реорганизацией организационно-штатной структуры объекта, увольнением служащих, имевших доступ к конфиденциальной информации и т. д.

- **Техника.** Пересмотр «Плана защиты» может быть вызван подключением других сетей, изменением или модификацией используемых средств вычислительной техники или программного обеспечения.

- **Помещения**. Пересмотр «Плана защиты» может быть вызван изменением территориального расположения компонентов объекта.

- **Документы**, регламентирующие деятельность по защите информации, оформляются в виде различных планов, положений, инструкций, наставлений и других аналогичных документов.

Контрольные вопросы.

- Перечислите виды защиты информации.
- Назовите объекты защиты информации и дайте их определения.
- Назовите способы защиты информации.
- Назовите свойства информации, составляющие модель информационной безопасности.
- Назовите основные принципы информационной безопасности.
- Перечислите условия и требования к защите информации.
- Дайте определения политики безопасности на объекте и сформулируйте требования, предъявляемые к плану защиты информации.

Литература

Основная:

1. Аполлонский А. В., Домбровская Л. А., Примакин А. И., Смирнова О. Г., Основы информационной безопасности в ОВД: Учебник для вузов. – СПб.: Университет МВД РФ, 2010.
2. Лопатин В. Н. Информационная безопасность России: Человек. Общество. Государство. Фонд «Университет». СПб 2000.

Дополнительная:

1. Васильев А.И., Сальников В.П., Степашин С.В. Национальная безопасность России: конституционное обеспечение. Фонд «Университет». СПб 1999.
2. Исмагилов Р.Ф., Сальников В.П., Степашин С.В. Экономическая безопасность России: концепция – правовые основы – политика. Фонд «Университет». СПб 2001.
3. Доценко С.М., Примакин А.И. Информационная безопасность и применение информационных технологий в борьбе с преступностью: Учебник для вузов. – СПб.: Университет МВД РФ, 2004.

Лекция разработана доцентом кафедры специальных информационных технологий полковником полиции Смирновой О.Г.