федеральное государственное бюджетное образовательное учреждение высшего образования «Красноярский государственный медицинский университет имени профессора В.Ф. Войно-Ясенецкого» Министерства здравоохранения Российской Федерации

УТВЕРЖДАЮ
Проректор по учебной работе, д.м.н., доцент
И.А. Соловьева
«20» октября 2021 г.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ
по дисциплине
Информационная безопасность
для подготовки обучающихся по направлению подготовки 38.04.02 Менеджмент, направленность (профиль) «Управление в здравоохранении на основе интеллектуального анализа данных»

Красноярск
2021

Практическое занятие №1

Тема: Правовые основы защиты информации в системе здравоохранения РФ.
Разновидность занятия: комбинированное.
Методы обучения: объяснительно-иллюстративный, репродуктивный, метод проблемного изложения, частично-поисковый, исследовательский.
Значение темы (актуальность изучаемой проблемы): освоение принципов информационной безопасности является одной из важнейших задач данной дисциплины. Выработка умений и навыков в использовании в сфере информационной безопасности необходима в практической работе будущего специалиста. Изучение данной темы позволит повысить уровень информационного сознания и культуры студентов.
Формируемые компетенции: ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2.
Место проведения и оснащение практического занятия: Компьютерный класс №6 (4-60/1) – видеопроектор, доска магнитно-маркерная, комплект учебной мебели на посадочные места, локальный сетевой сервер, персональные компьютеры, экран.
Структура содержания темы (хронокарта практического занятия)

п/п	Этапы практического занятия	Продолжительность (мин.)	Содержание этапа и оснащенность
1	Организация занятия	5.00	Проверка посещаемости и внешнего вида обучающихся
2	Формулировка темы и целей	20.00	Озвучивание преподавателем темы и ее актуальности, целей занятия
3	Контроль исходного уровня знаний и умений	20.00	Тестирование, индивидуальный устный или письменный опрос, фронтальный опрос
4	Раскрытие учебно-целевых вопросов по теме занятия	20.00	Изложение основных положений темы
5	Самостоятельная работа обучающихся (текущий контроль)	90.00	Выполнение практического задания
6	Итоговый контроль знаний (письменно или устно)	20.00	Тесты по теме, ситуационные задачи
7	Задание на дом (на следующее занятие)	5.00	Учебно-методические разработки следующего занятия и методические разработки для внеаудиторной работы по теме

	ВСЕГО	180	

Аннотация (краткое содержание темы):

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры. Информационная безопасность не сводится исключительно к защите информации. Субъект информационных отношений может пострадать (понести убытки) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в обслуживании клиентов. Более того, для многих открытых организаций (например, учебных) собственно защита информации не стоит на первом месте.

Для того чтобы освоить основы обеспечения информационной безопасности, необходимо владеть понятийным аппаратом. Раскрытие некоторых ключевых терминов не самоцель, важно формирование начальных представлений о целях и задачах защиты информации.

Под безопасностью информации понимается такое ее состояние, при котором исключается возможность просмотра, изменения или уничтожения информации лицами, не имеющими на это права, а также утечки информации за счет побочных электромагнитных излучений и наводок, специальных устройств перехвата (уничтожения) при передаче между объектами вычислительной техники.

Защита информации – это совокупность мероприятий, направленных на обеспечение конфиденциальности и целостности обрабатываемой информации, а также доступности информации для пользователей.

Конфиденциальность – сохранение в секрете критичной информации, доступ к которой ограничен узким кругом пользователей (отдельных лиц или организаций).

Целостность – свойство, при наличии которого информация сохраняет заранее определенные вид и качество.

Доступность – такое состояние информации, когда она находится в том виде, месте и времени, которые необходимы пользователю, и в то время, когда она ему необходима.

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

Правовые основы информационной безопасности

Законодательные меры в сфере информационной безопасности направлены на создание в стране законодательной базы, упорядочивающей и регламентирующей поведение субъектов и объектов информационных отношений, а также определяющей ответственность за нарушение установленных норм.

Работа по созданию нормативной базы предусматривает разработку новых или корректировку существующих законов, положений, постановлений и инструкций, а также создание действенной системы контроля за исполнением указанных документов. Необходимо отметить, что такая работа в последнее время ведется практически непрерывно, поскольку сфера информационных технологий развивается стремительно, соответственно появляются новые формы информационных отношений, существование которых должно быть определено законодательно.

Законодательная база в сфере информационной безопасности включает пакет Федеральных законов, Указов Президента РФ, постановлений Правительства РФ, межведомственных руководящих документов и стандартов.

Основополагающими документами по информационной безопасности в РФ являются Конституция РФ и Концепция национальной безопасности.

В Конституции РФ гарантируется «тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» (ст. 23, ч.2), а также «право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (ст. 29, ч.4). Кроме этого, Конституцией РФ «гарантируется свобода массовой информации» (ст. 29, ч.5), т. е. массовая информация должна быть доступна гражданам.

Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации

Закон Российской Федерации от 21 июля 1993 года №5485-1 «О государственной тайне» (ред от 08. 11.2011) с изменениями и дополнениями, внесенными после его принятия, регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

В Законе определены следующие основные понятия:

- государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
- носители сведений, составляющих государственную тайну, — материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;
- система защиты государственной тайны — совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;
- доступ к сведениям, составляющим государственную тайну — санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

- гриф секретности — реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;
- средства защиты информации — технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Законом определено, что средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на Государственную техническую комиссию при Президенте Российской Федерации, Федеральную службу безопасности Российской Федерации, Министерство обороны Российской Федерации в соответствии с функциями, возложенными на них законодательством Российской Федерации.

Закон РФ «Об информации, информационных технологиях и о защите информации» от 27. 07. 2006 №149-ФЗ (ред. от 02.07.2013) — является одним из основных базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

Согласно закону «Об информации, информационных технологиях и о защите информации», защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Приказом ФСТЭК России от 11.02.2013 №17 "Об утверждений Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" устанавливаются требования к обеспечению защиты информации от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в государственных информационных системах.

Ответственность за нарушения в сфере информационной безопасности

Немаловажная роль в системе правового регулирования информационных отношений отводится ответственности субъектов за нарушения в сфере информационной безопасности.

В сфере информационной безопасности устанавливается дисциплинарная, административная и уголовная ответственность.

Дисциплинарную ответственность за проступки в информационной сфере несут работники предприятий, учреждений, организаций в соответствии с положениями, уставами, правилами внутреннего трудового распорядка и другими нормативными актами.

Статьей 192 Трудового кодекса РФ от 30 декабря 2001 (ред. от 23.07.2013) г. установлено, что за совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания:

- замечание;
- выговор;
- увольнение по соответствующим основаниям.

Говоря об административной ответственности в области информационной безопасности, необходимо отметить, что в гл. 13 КоАП РФ предусмотрена ответственность за: нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11), нарушение правил защиты информации (ст. 13.12), незаконную деятельность в области защиты информации (ст. 13.13), разглашение информации с ограниченным доступом (ст. 13.14).

В принятом в 1996 г. Уголовном кодексе Российской Федерации (ред. от 21.10.2013), как наиболее сильнодействующем законодательном акте по предупреждению преступлений и привлечению преступников и нарушителей к уголовной ответственности, вопросам безопасности информации посвящены следующие главы и статьи:

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

Статья 140. Отказ в предоставлении гражданину информации.

Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей.

Статья 283. Разглашение государственной тайны.

Статья 284. Утрата документов, содержащих государственную тайну.

Особое внимание уделяется компьютерным преступлениям, ответственность за которые предусмотрена в специальной 28 главе кодекса «Преступления в сфере компьютерной информации». Глава 28 включает следующие статьи:

Статья 272. Неправомерный доступ к компьютерной информации.

Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, — наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, — наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или другого дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, — наказывается лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

Те же деяния, повлекшие по неосторожности тяжкие последствия, — наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, — наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

То же деяние, повлекшее по неосторожности тяжкие последствия, — наказывается лишением свободы на срок до четырех лет.

Примерная тематика НИРС по теме

1. Искусственный интеллект в информационной безопасности.
2. Искусственный интеллект: возможности и угрозы.
3. Как технологии искусственного интеллекта могут противостоять кибератакам?

Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2019. - 336 с. - Высшее образование. - Текст : электронный.

Дополнительная литература

1. Омельченко, В. П. Медицинская информатика : учебник / В. П. Омельченко, А. А. Демидова. - Москва : ГЭОТАР-Медиа, 2016. - Текст : электронный.
2. Медицинская информатика : учебник / ред. Т. В. Зарубина, Б. А. Кобринский. - 2-е изд., перераб. и доп. - Москва : ГЭОТАР-Медиа, 2022. - 464 с. - Текст : электронный.
3. Обмачевская, С. Н. Медицинская информатика. Курс лекций : учебное пособие для вузов / С. Н. Обмачевская. - 4-е изд., стер. - Санкт-Петербург : Лань, 2022. - 184 с. - Текст : электронный.
4. Советов, Б. Я. Информационные технологии : учебник для вузов / Б. Я. Советов, В. В. Цехановский. - 7-е изд., перераб. и доп. - М. : Юрайт , 2021. - 327 с. - Текст : электронный.
5. Гаврилов, М. В. Информатика и информационные технологии : учебник для вузов / М. В. Гаврилов, В. А. Климов. - 4-е изд., перераб. и доп. - Москва : Юрайт, 2021. - 383 с. - Текст : электронный.

Электронные ресурсы

1. Лекции по информационной безопасности (http://course.secsem.ru/lections)
2. Информатика для начинающих. Видеолекции (https://www.youtube.com/playlist?list=PLho0jPYl5RAEDNZnWd-xFfnIDvLJQ7FES)
3. Кибер-безопасность и десять сфер ее применения. Дистанционный курс (https://www.coursera.org/learn/cyber-security-domain)
4. Единый портал электронной подписи (www.iecp.ru)

Практическое занятие №2

Тема: Принципы обеспечения информационной безопасности. Условия успешного функционирования информационной системы. (В интерактивной форме).

Разновидность занятия: комбинированное.

Методы обучения: объяснительно-иллюстративный, репродуктивный, метод проблемного изложения, частично-поисковый, исследовательский.

Значение темы (актуальность изучаемой проблемы): освоение принципов информационной безопасности является одной из важнейших задач данной дисциплины. Выработка умений и навыков в использовании в сфере информационной безопасности необходима в практической работе будущего специалиста. Изучение данной темы позволит повысить уровень информационного сознания и культуры студентов.

Формируемые компетенции: ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2.

Место проведения и оснащение практического занятия: Компьютерный класс №6 (4-60/1) – видеопроектор, доска магнитно-маркерная, комплект учебной мебели на посадочные места, локальный сетевой сервер, персональные компьютеры, экран.

Структура содержания темы (хронокарта практического занятия)

п/п	Этапы практического занятия	Продолжительность (мин.)	Содержание этапа и оснащенность
1	Организация занятия	5.00	Проверка посещаемости и внешнего вида обучающихся
2	Формулировка темы и целей	20.00	Озвучивание преподавателем темы и ее актуальности, целей занятия
3	Контроль исходного уровня знаний и умений	20.00	Тестирование, индивидуальный устный или письменный опрос, фронтальный опрос
4	Раскрытие учебно-целевых вопросов по теме занятия	20.00	Изложение основных положений темы
5	Самостоятельная работа обучающихся (текущий контроль)	90.00	Выполнение практического задания
6	Итоговый контроль знаний (письменно или устно)	20.00	Тесты по теме, ситуационные задачи
7	Задание на дом (на следующее занятие)	5.00	Учебно-методические разработки следующего занятия и методические разработки для

			внеаудиторной работы по теме
	ВСЕГО	180	

Аннотация (краткое содержание темы):

В 1975 году Джерри Зальцер и Майкл Шрёдер в статье «Защита информации в компьютерных системах» впервые предложили разделить нарушения безопасности на три основных категории: неавторизованное раскрытие информации, неавторизованное изменение информации (и неавторизованный отказ в доступе к информации. Позднее эти категории получили краткие наименования и стандартизированные определения:

- «конфиденциальность» — свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов;
- «целостность» — свойство сохранения правильности и полноты активов;
- «доступность» — свойство информации быть доступной и готовой к использованию по запросу авторизованного субъекта, имеющего на это право.

В совокупности эти три ключевых принципа информационной безопасности именуются триадой CIA.

В 1992 году ОЭСР опубликовала свою собственную модель информационной безопасности, состоящую из девяти принципов: осведомлённость, ответственность, противодействие, этика, демократия, оценка риска, разработка и внедрение безопасности, управление безопасностью, пересмотр. В 1996 году на основе публикации ОЭСР 1992 года американский Национальный институт стандартов и технологий (NIST) сформулировал восемь основных принципов, которые гласят, что компьютерная безопасность «поддерживает миссию организации», «является неотъемлемой составляющей рационального менеджмента», «должна быть экономически эффективной», «требует всеобъемлющего и комплексного подхода», «ограничивается социальными факторами», «должна периодически подвергаться пересмотру», «обязанности и ответственность за компьютерную безопасность должны быть чётко сформулированы», а «владельцы систем несут ответственность за безопасность за пределами своей организации». На основе этой модели в 2004 году NIST опубликовал 33 принципа инженерного проектирования систем информационной безопасности, для каждого из которых были разработаны практические руководства и рекомендации, которые по сей день постоянно развиваются и поддерживаются в актуальном состоянии.

В 1998 году Донн Паркер дополнил классическую триаду CIA ещё тремя аспектами: владение или контроль, аутентичность и полезность. Достоинства этой модели, получившей название Паркеровская гексада, являются предметом дискуссий среди специалистов по информационной безопасности.

В 2009 году министерство обороны США опубликовало «Три основополагающих принципа компьютерной безопасности»: подверженность

системы [риску], доступность уязвимости и способность эксплуатировать уязвимость.

В 2011 году международный консорциум The Open Group опубликовал стандарт управления информационной безопасностью O-ISM3, в котором отказался от концептуального определения компонентов классической триады CIA в пользу их операционального определения. Согласно O-ISM3, для каждой организации можно идентифицировать индивидуальный набор целей безопасности, относящихся к одной из пяти категорий, которые соответствуют тому или иному компоненту триады: приоритетные цели безопасности (конфиденциальность), долгосрочные цели безопасности (целостность), цели качества информации (целостность), цели контроля доступа (доступность) и технические цели безопасности.

Из всех упомянутых выше моделей информационной безопасности классическая триада CIA по-прежнему остаётся наиболее признанной и распространённой в международном профессиональном сообществе. Она зафиксирована в национальных и международных стандартах и вошла в основные образовательные и сертификационные программы по информационной безопасности, такие как CISSP и CISM. Некоторые российские авторы используют кальку с него — «триада КЦД». В литературе все её три составляющих: конфиденциальность, целостность и доступность синонимически упоминаются, как принципы, атрибуты безопасности, свойства, фундаментальные аспекты, информационные критерии, важнейшие характеристики или базовые структурные элементы.

Между тем, в профессиональном сообществе не прекращаются дебаты о соответствии триады CIA стремительно развивающимся технологиям и требованиям бизнеса. В результате этих дискуссий появляются рекомендации о необходимости установки взаимосвязи между безопасностью и неприкосновенностью частной жизни, а также утверждения дополнительных принципов. Некоторые из них уже включены в стандарты Международной организации по стандартизации (ISO):

- подлинность — свойство, гарантирующее, что субъект или ресурс идентичны заявленному;
- подотчётность — ответственность субъекта за его действия и решения;
- невозможность отказа — способность удостоверять имевшее место событие или действие и их субъекты так, чтобы это событие или действие и субъекты, имеющие к нему отношение, не могли быть поставлены под сомнение;
- достоверность — свойство соответствия предусмотренному поведению и результатам.

Конфиденциальность

Конфиденциальность информации достигается предоставлением к ней доступа с наименьшими привилегиями исходя из принципа минимальной необходимой осведомлённости. Иными словами, авторизованное лицо должно иметь доступ только к той информации, которая ему необходима для исполнения своих должностных обязанностей. Упомянутые выше

преступления против неприкосновенности частной жизни, такие, как кража личности, являются нарушениями конфиденциальности. Одной из важнейших мер обеспечения конфиденциальности является классификация информации, которая позволяет отнести её к строго конфиденциальной, или предназначенной для публичного, либо внутреннего пользования. Шифрование информации — характерный пример одного из средств обеспечения конфиденциальности.

Целостность

Чёткое осуществление операций или принятие верных решений в организации возможно лишь на основе достоверных данных, хранящихся в файлах, базах данных или системах, либо транслируемых по компьютерным сетям. Иными словами, информация должна быть защищена от намеренного, несанкционированного или случайного изменения по сравнению с исходным состоянием, а также от каких-либо искажений в процессе хранения, передачи или обработки. Однако её целостности угрожают компьютерные вирусы и логические бомбы, ошибки программирования и вредоносные изменения программного кода, подмена данных, неавторизованный доступ, бэкдоры и тому подобное. Помимо преднамеренных действий, во многих случаях неавторизованные изменения важной информации возникают в результате технических сбоев или человеческих ошибок по оплошности или из-за недостаточной профессиональной подготовки. Например, к нарушению целостности ведут: случайное удаление файлов, ввод ошибочных значений, изменение настроек, выполнение некорректных команд, причём, как рядовыми пользователями, так и системными администраторами.

Для защиты целостности информации необходимо применение множества разнообразных мер контроля и управления изменениями информации и обрабатывающих её систем. Типичным примером таких мер является ограничение круга лиц с правами на изменения лишь теми, кому такой доступ необходим для выполнения служебных обязанностей. При этом следует соблюдать принцип разграничения полномочий, согласно которому изменения в данные или информационную систему вносит одно лицо, а подтверждает их или отклоняет — другое. Кроме того, любые изменения в ходе жизненного цикла информационных системы должны быть согласованны, протестированы на предмет обеспечения информационной целостности и внесены в систему только корректно сформированными транзакциями. Обновления программного обеспечения необходимо производить с соблюдением мер безопасности. Любые действия, влекущие изменения, должны быть обязательно протоколированы.

Доступность

Согласно этому принципу, информация должна быть доступна авторизованным лицам, когда это необходимо. Основными факторами, влияющими на доступность информационных систем, являются DoS-атаки, атаки программ-вымогателей, саботаж. Кроме того, источником угроз доступности являются непреднамеренные человеческие ошибки по оплошности или из-за недостаточной профессиональной подготовки:

случайное удаление файлов или записей в базах данных, ошибочные настройки систем; отказ в обслуживании в результате превышения допустимой мощности или недостатка ресурсов оборудования, либо аварий сетей связи; неудачно проведённое обновление аппаратного или программного обеспечения; отключение систем из-за аварий энергоснабжения. Существенную роль в нарушении доступности играют также природные катастрофы: землетрясения, смерчи, ураганы, пожары, наводнения и тому подобные явления. Во всех случаях конечный пользователь теряет доступ к информации, необходимой для его деятельности, возникает вынужденный простой. Критичность системы для пользователя и её важность для выживания организации в целом определяют степень воздействия времени простоя. Недостаточные меры безопасности увеличивают риск поражения вредоносными программами, уничтожения данных, проникновения извне или DoS-атак. Подобные инциденты могут сделать системы недоступными для обычных пользователей.

Информационная система - система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию (ISO/IEC 2382:2015).

Информационная безопасность ИС является обязательной. При автоматизации степень защищенности является одной из характеристик информационной системы.

Необходимость защиты информации возрастает при широком использовании средств автоматизации и электронных носителей информации. Информация в электронном виде более подвержена различным угрозам. Ее легче скопировать, уничтожить, исказить, чем информацию на бумажных носителях. К обычным видам угроз (пожар, стихийное бедствие, хищение) добавляются многие другие.

Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ в статье 16 устанавливает понятие защиты информации.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Государство регулирует отношения в сфере защиты информации, устанавливает требования к защите информации, ответственность за нарушение законодательства.

Обладатель информации, оператор информационной системы обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствии нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

В соответствии с Федеральным законом «О персональных данных» № 152-ФЗ любая организация, которая собирает, хранит, обрабатывает персональные данные, в том числе фамилию, имя, отчество, дату рождения, другие паспортные данные, должна обеспечить защиту этих данных, защиту прав на неприкосновенность частной жизни, личную и семейную тайну.

Под безопасностью информационной системы понимается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования.

Утрата документов, баз данных, может вызвать не только остановку работы предприятия, но и невозможность ее возобновления в дальнейшем, а несанкционированный доступ к информации - ослабление позиций предприятия по сравнению с конкурентами.

Многие информационные системы, например, банков, военных и государственных организаций, где утечка и утрата информации недопустима, должны быть защищены очень надежно.

Объектами защиты в информационной системе являются не только информационные ресурсы. Для обеспечения нормальной работы АИС и защиты информации необходимо защищать и другие компоненты информационной системы: технические средства, программы, сети.

Примерная тематика НИРС по теме

1. Искусственный интеллект и анализ данных.
2. Искусственный интеллект – прорывная технология в информационной безопасности.
3. Почему искусственный интеллект все чаще принимают на кибервооружение?

Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2019. - 336 с. - Высшее образование. - Текст : электронный.

Дополнительная литература

1. Омельченко, В. П. Медицинская информатика : учебник / В. П. Омельченко, А. А. Демидова. - Москва : ГЭОТАР-Медиа, 2016. - Текст : электронный.
2. Медицинская информатика : учебник / ред. Т. В. Зарубина, Б. А. Кобринский. - 2-е изд., перераб. и доп. - Москва : ГЭОТАР-Медиа, 2022. - 464 с. - Текст : электронный.
3. Обмачевская, С. Н. Медицинская информатика. Курс лекций : учебное пособие для вузов / С. Н. Обмачевская. - 4-е изд., стер. - Санкт-Петербург : Лань, 2022. - 184 с. - Текст : электронный.
4. Советов, Б. Я. Информационные технологии : учебник для вузов / Б. Я. Советов, В. В. Цехановский. - 7-е изд., перераб. и доп. - М. : Юрайт , 2021. - 327 с. - Текст : электронный.
5. Гаврилов, М. В. Информатика и информационные технологии : учебник для вузов / М. В. Гаврилов, В. А. Климов. - 4-е изд., перераб. и доп. - Москва : Юрайт, 2021. - 383 с. - Текст : электронный.

Электронные ресурсы

1. Лекции по информационной безопасности (http://course.secsem.ru/lections)
2. Информатика для начинающих. Видеолекции (https://www.youtube.com/playlist?list=PLho0jPYl5RAEDNZnWd-xFfnIDvLJQ7FES)
3. Кибер-безопасность и десять сфер ее применения. Дистанционный курс (https://www.coursera.org/learn/cyber-security-domain)
4. Единый портал электронной подписи (www.iecp.ru)

Практическое занятие №3

Тема: Направления защиты информации в ИС. Основные виды угроз безопасности ИС и информации. (В интерактивной форме).

Разновидность занятия: комбинированное.

Методы обучения: объяснительно-иллюстративный, репродуктивный, метод проблемного изложения, частично-поисковый, исследовательский.

Значение темы (актуальность изучаемой проблемы): освоение принципов информационной безопасности является одной из важнейших задач данной дисциплины. Выработка умений и навыков в использовании в сфере информационной безопасности необходима в практической работе будущего специалиста. Изучение данной темы позволит повысить уровень информационного сознания и культуры студентов.

Формируемые компетенции: ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2.

Место проведения и оснащение практического занятия: Компьютерный класс №6 (4-60/1) – видеопроектор, доска магнитно-маркерная, комплект учебной мебели на посадочные места, локальный сетевой сервер, персональные компьютеры, экран.

Структура содержания темы (хронокарта практического занятия)

п/п	Этапы практического занятия	Продолжительность (мин.)	Содержание этапа и оснащенность
1	Организация занятия	5.00	Проверка посещаемости и внешнего вида обучающихся
2	Формулировка темы и целей	20.00	Озвучивание преподавателем темы и ее актуальности, целей занятия
3	Контроль исходного уровня знаний и умений	20.00	Тестирование, индивидуальный устный или письменный опрос, фронтальный опрос
4	Раскрытие учебно-целевых вопросов по теме занятия	20.00	Изложение основных положений темы
5	Самостоятельная работа обучающихся (текущий контроль)	90.00	Выполнение практического задания
6	Итоговый контроль знаний (письменно или устно)	20.00	Тесты по теме, ситуационные задачи
7	Задание на дом (на следующее занятие)	5.00	Учебно-методические разработки следующего занятия и методические разработки для внеаудиторной работы по теме

	ВСЕГО	180	

Аннотация (краткое содержание темы):

Направления обеспечения безопасности информационных систем представляют собой совокупность комплексных мер, направленных на предотвращение угроз информационным системам на различных уровнях.

Выделяют защиту правовую, организационную, инженерно-техническую.

Правовая защита информации заключается в разработке нормативных правовых актов, регламентирующих отношения, возникающие при осуществлении права на поиск, получение, передачу и распространение информации, применении информационных технологий, производство обеспечение защиты информации.

Базовым законодательным актом в сфере защиты информации является Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 25.11.2017). Указанный закон регулирует отношения, связанные с осуществлением права на поиск, получение, передачу, производство и распространение информации, применением информационных технологий; обеспечением гарантия защиты информации Он разделяет информацию на информацию, доступ к которой ограничен законодательством и общедоступную.

Система законодательных актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного доступа за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты.

Всего в российском законодательстве насчитывается более 30 видов тайн. Сотрудникам органов внутренних дел наиболее часто приходится сталкиваться с защитой следующих видов тайн: государственная, служебная, правовая, следствия, тайна сведений о защищаемом лице, персональные данные и др.

За преступления и правонарушения в сфере защиты информации действующим законодательством установлена уголовная и административная ответственность. Например, уголовная ответственность установлена за государственную измену (шпионаж) в форме выдачи государственной тайны, разглашение государственной тайны. Административная ответственность наступает за нарушение установленного законом порядка сбора, хранения, использования или распространения, а также порядка предоставления (непредставление или предоставление ложных сведений) информации; нарушение правил защиты информации, незаконная деятельность в области защиты информации, разглашение информации с ограниченным доступом (например, о мерах безопасности) и другие составы административных правонарушений, закрепленных в главе 13 КоАП РФ

Организационная защита - это регламентация служебной деятельности и взаимоотношений сотрудников на нормативно-правовой основе,

исключающей или значительно затрудняющей неправомерное овладение информацией ограниченного доступа и проявление внутренних и внешних угроз.

К основным организационным мероприятиям можно отнести:

- организацию режима и охраны с целью исключения возможности несанкционированного проникновения на территорию и в помещения посторонних лиц, контроля прохода на территорию сотрудников и посетителей,
- организацию защищенного документооборота;
- организацию работы по допуску сотрудников к информации ограниченного доступа,
- организацию использования технических средств сбора, передачи и хранения информации ограниченного доступа, организацию работы по анализу внутренних и внешних угроз информации ограниченного доступа;
- организацию работ по проведению систематического контроля за сотрудниками, работающими с документами ограниченного доступа.

Инженерно-техническая защита информации - это совокупность специальных технических средств и мероприятий по их использованию с целью защиты информации ограниченного доступа.

По функциональному назначению средства инженерно-технической защиты информации классифицируются на следующие группы:

- физические средства, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям информации ограниченного доступа и осуществляющие защиту сотрудников, материальных средств и информации от противоправных воздействий;
- аппаратные средства включают в себя приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации с целью гарантированной защиты информации от утечки, разглашения и несанкционированного доступа,
- программные средства, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки данных;
- криптографические средства с помощью специальных математических алгоритмов производят преобразование информации, передаваемой по линиям связи или хранящейся в технических средствах, таким образом, что при несанкционированном доступе злоумышленник не имеет возможности ознакомиться с содержанием передаваемой или хранимой информации.

Под угрозой безопасности информации понимают события или действия, которые могут привести к искажению, несанкционированному

использованию, разрушению информационных ресурсов, а также программных и технических средств.

Случайные угрозы - возникают независимо от воли и желания людей. Их источником могут быть неисправности технических средств, ошибки персонала, ошибки в программном обеспечении.

Умышленные, преднамеренные угрозы преследуют цель нанесения ущерба управляемой системе или пользователям.

Виды умышленных угроз:

- Пассивные угрозы направлены в основном на несанкционированное использование информационных ресурсов информационной системы, не оказывая при этом влияния на ее функционирование. Например, несанкционированный доступ к базам данных, копирование данных, прослушивание линий связи.
- Активные угрозы имеют целью нарушение нормального функционирования информационной системы. К ним относятся, например, вывод из строя компьютера или программного обеспечения, искажение и уничтожение информации в базах данных, нарушение работы линий связи.

Угрозы подразделяются на внутренние и внешние.

- Внутренние - возникают внутри организации, исходят чаще всего от персонала.
- Внешние - возникают извне. Это могут быть злонамеренные действия конкурентов, промышленный шпионаж.

Особое значение приобрела угроза от вредоносных программ и вирусов. Практически каждый пользователь сталкивается с вирусами, с различными нарушениями в работе программных средств, вызываемыми ими, другими последствиями. С развитием компьютерных сетей значение этой угрозы возрастает. Существуют вирусы (черви), распространяющиеся по электронной почте, рассылающие сами себя по всем имеющимся в системе адресам.

Вредоносные программы бывают и других типов. Логические бомбы используются в основном для разрушения или искажения информации. Внедренные злоумышленниками, они начинают действовать при наступлении определенных условий.

Троянский конь - программа, выполняющая в дополнение к основным действиям дополнительные, не описанные в документации. Представляет собой дополнительный блок команд, вставленный в исходную безвредную программу.

Захватчик паролей - программы, предназначенные для воровства паролей.

Основными угрозами безопасности информации являются:

- неправильные действия пользователя. Это могут быть неправильно введенные данные, команды, ошибки администрирования. Они могут привести к уничтожению, разрушению, искажению информации;

- неисправности, сбои технических и программных средств, аварии нарушают нормальную работу информационной системы, могут приводить к потерям информации;
- вирусы и вредоносные программы представляют серьезную угрозу, но при правильном применении средств защиты угроза может быть сведена к минимуму;
- кражи технических средств и носителей информации;
- несанкционированный доступ к ресурсам может привести как к нарушению нормальной работы информационной системы, утрате информации, так и к несанкционированному использованию информации с целью нанесения ущерба, обогащения. Такой доступ может быть осуществлен путем входа в систему под чужим именем, прослушивания линий связи, регистрации излучений от технических средств и другими способами.

Реализация угроз ИС приводит к различным видам прямых или косвенных потерь. Материальный ущерб может возникать при утрате имущества, необходимости ремонтных работ, расходов на восстановление информации и др. Потери могут выражаться в ущемлении интересов, потере клиентов, ухудшении положения на рынке.

Примерная тематика НИРС по теме

1. Нужна ли защита для искусственного интеллекта?
2. Робот-хакер.

Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2019. - 336 с. - Высшее образование. - Текст : электронный.

Дополнительная литература

1. Омельченко, В. П. Медицинская информатика : учебник / В. П. Омельченко, А. А. Демидова. - Москва : ГЭОТАР-Медиа, 2016. - Текст : электронный.
2. Медицинская информатика : учебник / ред. Т. В. Зарубина, Б. А. Кобринский. - 2-е изд., перераб. и доп. - Москва : ГЭОТАР-Медиа, 2022. - 464 с. - Текст : электронный.
3. Обмачевская, С. Н. Медицинская информатика. Курс лекций : учебное пособие для вузов / С. Н. Обмачевская. - 4-е изд., стер. - Санкт-Петербург : Лань, 2022. - 184 с. - Текст : электронный.
4. Советов, Б. Я. Информационные технологии : учебник для вузов / Б. Я. Советов, В. В. Цехановский. - 7-е изд., перераб. и доп. - М. : Юрайт , 2021. - 327 с. - Текст : электронный.
5. Гаврилов, М. В. Информатика и информационные технологии : учебник для вузов / М. В. Гаврилов, В. А. Климов. - 4-е изд., перераб. и доп. - Москва : Юрайт, 2021. - 383 с. - Текст : электронный.

Электронные ресурсы

1. Лекции по информационной безопасности (http://course.secsem.ru/lections)
2. Информатика для начинающих. Видеолекции (https://www.youtube.com/playlist?list=PLho0jPYl5RAEDNZnWd-xFfnIDvLJQ7FES)
3. Кибер-безопасность и десять сфер ее применения. Дистанционный курс (https://www.coursera.org/learn/cyber-security-domain)
4. Единый портал электронной подписи (www.iecp.ru)

Практическое занятие №4

Тема: Методы и технологии защиты информации, конфиденциальности информации в информационных системах. Технологии защиты целостности информации. Методы и технологии защиты доступности информации. (В интерактивной форме).

Разновидность занятия: комбинированное.

Методы обучения: объяснительно-иллюстративный, репродуктивный, метод проблемного изложения, частично-поисковый, исследовательский.

Значение темы (актуальность изучаемой проблемы): освоение принципов информационной безопасности является одной из важнейших задач данной дисциплины. Выработка умений и навыков в использовании в сфере информационной безопасности необходима в практической работе будущего специалиста. Изучение данной темы позволит повысить уровень информационного сознания и культуры студентов.

Формируемые компетенции: ПК-2.2, УК-7.1, УК-7.2, УК-7.6, ОПК-12.2.

Место проведения и оснащение практического занятия: Компьютерный класс №6 (4-60/1) – видеопроектор, доска магнитно-маркерная, комплект учебной мебели на посадочные места, локальный сетевой сервер, персональные компьютеры, экран.

Структура содержания темы (хронокарта практического занятия)

п/п	Этапы практического занятия	Продолжительность (мин.)	Содержание этапа и оснащенность
1	Организация занятия	5.00	Проверка посещаемости и внешнего вида обучающихся
2	Формулировка темы и целей	20.00	Озвучивание преподавателем темы и ее актуальности, целей занятия
3	Контроль исходного уровня знаний и умений	20.00	Тестирование, индивидуальный устный или письменный опрос, фронтальный опрос
4	Раскрытие учебно-целевых вопросов по теме занятия	20.00	Изложение основных положений темы
5	Самостоятельная работа обучающихся (текущий контроль)	90.00	Выполнение практического задания
6	Итоговый контроль знаний (письменно или устно)	20.00	Тесты по теме, ситуационные задачи
7	Задание на дом (на следующее занятие)	5.00	Учебно-методические разработки следующего занятия и

			методические разработки для внеаудиторной работы по теме
	ВСЕГО	180	

Аннотация (краткое содержание темы):

Методы защиты конфиденциальности информации

Конфиденциальность информации - параметр информации определяющие её неразглашение третьему кругу лиц.

Как следует из определения конфиденциальная информация это информация ограниченного доступа, соответственно методы её защиты заключаются в невозможности доступа злоумышленников к этой информации. Для того чтобы эту информацию получить злоумышленник использует атаку доступа.

Атака доступа - это попытка получения злоумышленником информации, для просмотра которой у него нет разрешений. Осуществление такой атаки возможно везде, где существует информация и средства для ее передачи.

Виды атак доступа:

Подсматривание (snooping) - это просмотр файлов или документов для поиска интересующей злоумышленника информации. Если информация находится в компьютерной системе, то он будет просматривать файл за файлом, пока не найдет нужные сведения.

Подслушивание

Когда кто-то слушает разговор, участником которого он не является, это называется подслушиванием (eavesdropping). Для получения несанкционированного доступа к информации злоумышленник должен находиться поблизости от нее. Очень часто при этом он использует электронные устройства

Внедрение беспроводных сетей увеличило вероятность успешного прослушивания. Теперь злоумышленнику не нужно находиться внутри системы или физически подключать подслушивающее устройство к сети. Вместо этого во время сеанса связи он располагается на стоянке для автомобилей или вблизи здания.

Перехват

В отличие от подслушивания перехват (interception) - это активная атака. Злоумышленник захватывает информацию в процессе ее передачи к месту назначения. После анализа информации он принимает решение о разрешении или запрете ее дальнейшего прохождения

Методы защиты:

1. Грамотная политика доступа к файлам, раздаваемая не автоматически, а в ручную, исходя из должности сотрудника и уровня допуска к файлам подлежащим защите.

2. Шифрование файлов являющихся конфиденциальной собственностью.

3. Ведение журнала аудита.

Выполнение атаки доступа на информацию находящуюся в электронном виде:

Информация в электронном виде хранится:

- на рабочих станциях
- на серверах
- в портативных компьютерах
- на флоппи-дисках
- на компакт-дисках
- на резервных магнитных лентах

Если злоумышленник имеет легальный доступ к системе, он будет анализировать файлы, просто открывая один за другим. При должном уровне контроля над разрешениями доступ для нелегального пользователя будет закрыт, а попытки доступа зарегистрированы в журналах аудита.

Правильно настроенные разрешения предотвратят случайную утечку информации (настройка политики безопасности компьютерной сети). Однако серьезный взломщик постарается обойти систему контроля и получить доступ к нужной информации. Существует большое количество уязвимых мест, которые помогут ему в этом.

При прохождении информации по сети к ней можно обращаться, прослушивая передачу. Взломщик делает это, устанавливая в компьютерной системе сетевой анализатор пакетов (sniffer). Обычно это компьютер, сконфигурированный для захвата всего сетевого трафика (не только трафика, адресованного данному компьютеру). Для этого взломщик должен повысить свои полномочия в системе или подключиться к сети. Анализатор настроен на захват любой информации, проходящей по сети, но особенно - на пользовательские идентификаторы и пароли так как в основном в системах на них выделяется фиксированное значение размера (при генерации паролей случайными символами), это значительно облегчает задачу, однако работает это только при условии статистической зависимости а значит легко устраняется методами шифрования подавляющими эту зависимость. Самый провальный вариант защиты информации от анализатора пакетов это дать пользователям создавать пароли самостоятельно при этом ещё и не используя шифрование всего трафика внутренней сети.

Как уже говорилось выше, появление беспроводной технологии позволяет взломщикам перехватывать трафик без физического доступа к системе. Беспроводные сигналы считываются на довольно большом расстоянии от их источника:

- на других этажах здания
- на автомобильной стоянке
- на улице рядом со зданием

Подслушивание выполняется и в глобальных компьютерных сетях типа выделенных линий и телефонных соединений. Однако такой тип перехвата требует наличия соответствующей аппаратуры и специальных знаний. В этом

случае наиболее удачным местом для размещения подслушивающего устройства является шкаф с электропроводкой.

Перехват возможен даже в системах оптико-волоконной связи с помощью специализированного оборудования (а конкретно с помощью делителей и ответвителей света, обнаружить, возможно, лишь используя сложнейшее оборудование способное зарегистрировать деградацию сигнала).

Информационный доступ с использованием перехвата - одна из сложнейших задач для злоумышленника. Чтобы добиться успеха, он должен поместить свою систему в линии передачи между отправителем и получателем информации. В интернете это выполняется посредством изменения разрешения имени, в результате чего имя компьютера преобразуется в неправильный адрес. Трафик перенаправляется к системе атакующего вместо реального узла назначения. Достигается это посредством внедрения вируса (мой случай), он проникает в систему и заменяет функцию получения DNS-сервера автоматически на использование определенного (предпочитаемого) DNS.

Методы защиты целостности информации

Целостность информации - параметр информации, определяющий, что после создания файла тот не был, подвергнут несанкционированным модификациям.

Для реализации угрозы целостности злоумышленники используют атаку модификации.

Атака модификации - это попытка неправомочного изменения информации. Такая атака возможна везде, где существует или передается информация; она направлена на нарушение целостности информации.

Виды атаки модификации:

Замена

Одним из видов атаки модификации является замена существующей информации, например, изменение номера банковской карты служащего, что приведет к переводу средств на счет злоумышленника. Атака замены направлена как против секретной, так и общедоступной информации. Это самый опасный вид атаки модификации, так как его реализация может привести к очень серьёзным последствиям.

Добавление

Добавление новых данных, например, в журнал аудита, при условии интеллектуального управления (smart journal) добавление записи разрешающей определенному пользователю некоторое действие, она будет проанализирована и этому пользователю будут присвоены более высокие полномочия (как пример внести запись о модификации документа для пользователя, не имеющего такой привилегией, или же вообще не существующего). При реализации модификации журнала аудита будет катастрофа.

Удаление

Атака удаления означает перемещение существующих данных, например, аннулирование записи об операции из балансового отчета банка, в результате чего снятые со счета денежные средства остаются на нем.

Методы защиты:

1. Хеширование документов, чья целостность находится под угрозой.
2. Использование цифровой подписи.
3. Тщательная работа с журналом аудита и отключение возможности внесения в него записей всеми кроме системного администратора.

Выполнение атаки модификации на информацию находящуюся в электронном виде:

Модифицировать, информацию, хранящуюся в электронном виде, значительно легче нежели просто похитить. Учитывая, что взломщик может заполучить доступ к системе, такая операция оставляет после себя минимум улик или не оставляет их вообще. При отсутствии санкционированного доступа к файлам атакующий сначала должен обеспечить себе вход в систему (чего можно добиться огромным количеством методов начиная социальной инженерии заканчивая грубым взлом с подбором) или удалить разрешения файла (для этого нужно заполучить определенные привилегии, для этого на выручку приходит либо журнал аудита, либо кража чужого профиля). Атаки такого рода используют уязвимые места систем, например, "backdoor" в безопасности сервера, позволяющие заменить домашнюю страницу.

Изменение файлов базы данных или списка транзакций должно выполняться очень осторожно. Транзакции нумеруются последовательно, и удаление или добавление неправильных операционных номеров будет замечено. В этих случаях необходимо будет основательно поработать во всей системе, чтобы воспрепятствовать обнаружению.

Труднее произвести успешную атаку модификации при передаче информации. Для этого нужно накладывать модификацию непосредственно на передаваемые биты по шаблону, это не даст слишком сильной просадки в скорости однако при грамотной работе специалиста на другом конце может быть обнаружено. Так же для этого метода необходимо заранее знать по какому шаблону будет отправляться информация, будь то запрос на регистрацию, или запрос от банка на подтверждение операции оплаты. Лучший способ - сначала выполнить перехват интересующего трафика, а затем внести изменения в информацию перед ее отправкой к пункту назначения. Однако это не самый лучший путь так как имеет один серьезный недостаток заключающийся в том что чаще всего отправляемые файлы уходят либо сразу после создания либо по частям во время создания.

Методы защиты доступности информации

Доступность информации - параметр информации, который определяет, что информация должна быть доступна в любой момент времени пользователю, обладающему привилегией на взаимодействие с ней.

Для реализации угрозы доступности информации злоумышленник использует атаку на отказ в обслуживании.

Атаки на отказ в обслуживании (Denial-of-service, DoS) - это атаки, запрещающие легальному пользователю использование системы, информации или возможностей компьютеров. В результате DoS-атаки злоумышленник обычно не получает доступа к компьютерной системе и не может оперировать с информацией. Однако это открывает перед злоумышленником легкий путь по дальнейшему взлому системы так как некоторые системы в нештатной ситуации могут выдать версию ПО или фрагмент программного кода. Так же экономически очень выгодна в борьбе с конкурентами, так как на восстановление работоспособности системы уйдет время и деньги, а виновник не понесет особых проблем связанных с законом.

Виды DoS атак

Отказ в доступе к информации

В результате DoS-атаки, направленной против информации, последняя становится непригодной для использования. Информация уничтожается, искажается или переносится в недоступное место.

Отказ в доступе к приложениям

Другой тип DoS-атак направлен на приложения, обрабатывающие или отображающие информацию, или на компьютерную систему, в которой эти приложения выполняются. В случае успеха подобной атаки решение задач, выполняемых с помощью такого приложения, становится невозможным.

Отказ в доступе к системе

Общий тип DoS-атак ставит своей целью вывод из строя компьютерной системы, в результате чего сама система, установленные на ней приложения и вся сохраненная информация становится недоступной.

Отказ в доступе к средствам связи

Атаки на отказ в доступе к средствам связи выполняются уже много лет. В качестве примера можно привести разрыв сетевого провода, глушение радиопередач или лавинную рассылку сообщений, создающую непомерный трафик. Целью атаки является коммуникационная среда. Целостность компьютерной системы и информации не нарушается, однако отсутствие средств связи лишает доступа к этим ресурсам.

Метод защиты:

1. Для защиты от сетевых атак применяется ряд фильтров, подключенных к интернет-каналу с большой пропускной способностью. Фильтры действуют таким образом, что последовательно анализируют проходящий трафик, выявляя нестандартную сетевую активность и ошибки. В число анализируемых шаблонов нестандартного трафика входят все известные на сегодняшний день методы атак, в том числе реализуемые и при помощи распределённых бот-сетей.

Выполнение DoS-атаки на информацию находящуюся в электронном виде:

Существует много способов выполнения DoS-атак, способных повредить информацию, хранящуюся в электронном виде. Ее можно удалить, а для закрепления успеха злоумышленник удалит и все резервные копии этой информации. Он может привести файл в негодность, зашифровав его и затем

уничтожив ключ шифрования. Доступ к информации будет потерян, если не существует резервной копии файла.

Физическая атака DoS - это и физическое уничтожение компьютера (или его кража). Пример кратковременной атаки DoS - отключение компьютера, в результате которого пользователи лишаются доступа к своим приложениям.

Существуют атаки DoS, нацеленные непосредственно на компьютерную систему. Они реализуются через эксплоиты, использующие уязвимые места операционных систем или межсетевых протоколов

Злоумышленникам хорошо известны и "backdoor" в приложениях. С их помощью атакующий посылает в приложение определенный набор команд, который оно не в состоянии правильно обработать, в результате чего приложение выходит из строя. Перезагрузка восстанавливает его работоспособность, но на время перезагрузки работать с приложением становится невозможно.

Самый легкий способ привести в нерабочее состояние средства коммуникации - это перерезать сетевой кабель. Для такой атаки требуется физический доступ к проводке, но, как мы увидим дальше, ковш экскаватора является мощным инструментом DoS-атак.

DoS-атаки, направленные на средства связи, выполняют отправку на сайт непомерно большого трафика. Этот трафик буквально переполняет коммуникационную инфраструктуру, лишая доступа к сети легальных пользователей.

Но не все DoS-атаки являются преднамеренными, иногда случайность играет большую роль в возникновении подобных инцидентов. Экскаватор, о котором я говорил выше, может оборвать оптико-волоконную линию передачи во время выполнения своей обычной работы. Такой обрыв уже служил поводом множества DoS-инцидентов для пользователей телефонных сетей и интернета. Разработчики, тестирующие новый программный код, иногда выводили из строя большие системы, совершенно того не желая. Даже дети становятся причиной случайной DoS-атаки. Во время экскурсии по центру обработки данных ребенок будет настолько очарован мерцающими повсюду огоньками, что не удержится от соблазна нажать на красивую кнопку - и остановит или перезагрузит всю систему.

Примерная тематика НИРС по теме

1. Стоит ли бояться искусственного интеллекта?
2. Медицина и искусственный интеллект: возможно ли это?

Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2019. - 336 с. - Высшее образование. - Текст : электронный.

Дополнительная литература

1. Омельченко, В. П. Медицинская информатика : учебник / В. П. Омельченко, А. А. Демидова. - Москва : ГЭОТАР-Медиа, 2016. - Текст : электронный.
2. Медицинская информатика : учебник / ред. Т. В. Зарубина, Б. А. Кобринский. - 2-е изд., перераб. и доп. - Москва : ГЭОТАР-Медиа, 2022. - 464 с. - Текст : электронный.
3. Обмачевская, С. Н. Медицинская информатика. Курс лекций : учебное пособие для вузов / С. Н. Обмачевская. - 4-е изд., стер. - Санкт-Петербург : Лань, 2022. - 184 с. - Текст : электронный.
4. Советов, Б. Я. Информационные технологии : учебник для вузов / Б. Я. Советов, В. В. Цехановский. - 7-е изд., перераб. и доп. - М. : Юрайт , 2021. - 327 с. - Текст : электронный.
5. Гаврилов, М. В. Информатика и информационные технологии : учебник для вузов / М. В. Гаврилов, В. А. Климов. - 4-е изд., перераб. и доп. - Москва : Юрайт, 2021. - 383 с. - Текст : электронный.

Электронные ресурсы

1. Лекции по информационной безопасности (http://course.secsem.ru/lections)
2. Информатика для начинающих. Видеолекции (https://www.youtube.com/playlist?list=PLho0jPYl5RAEDNZnWd-xFfnIDvLJQ7FES)
3. Кибер-безопасность и десять сфер ее применения. Дистанционный курс (https://www.coursera.org/learn/cyber-security-domain)
4. Единый портал электронной подписи (www.iecp.ru)