**Тема 1: "ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ"**

***1.1 Понятие информационной безопасности***

Информация – самый ценный ресурс в компании, а в некоторых случаях является и производственным ресурсом, от сохранности которого зависят важные технологические процессы. С развитием информационных технологий увеличивается риск утечки информации, заражение вирусами, вмешательства в работу системы.

Информация существует в различных формах. Ее можно хранить на компьютерах, передавать по вычислительным сетям, распечатывать или записывать на бумаге, а также озвучивать в разговорах. С точки зрения безопасности все виды информации, включая бумажную документацию, базы данных, пленки, микрофильмы, модели, магнитные ленты, дискеты, разговоры и другие способы, используемые для передачи знаний и идей, требуют надлежащей защиты.

Защитные меры оказываются значительно более дешевыми и эффективными, если они встроены в информационные системы и сервисы на стадиях задания требований и проектирования. Чем скорее организация примет меры по защите своих информационных систем, тем более дешевыми и эффективными они будут для нее впоследствии.

Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл.

*В широком смысле информационная безопасность (ИБ) это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.*

В данном курсе наше внимание будет сосредоточено на хранении, обработке и передаче информации вне зависимости от того, каким образом она закодирована, кто или что является ее источником. Поэтому термин «информационная безопасность» будет использоваться в узком смысле.

Под информационной безопасностью в узком смысле мы будем понимать *защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.*

*Защита информации это комплекс мероприятий, направленных на обеспечение информационной безопасности.*

***1.2 Объект защиты информации***

**Объектом защиты информации** является информационная система (предприятия, коммерческой организации) или автоматизированная система обработки данных. Что же понимается под этим термином?

В большинстве изданий по ИБ под ИС понимается *комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации.*

Наряду с термином "информация" применительно к ИС часто используют термин "данные". Используется и другое понятие "информационные ресурсы".

**Под информационными ресурсами** понимаются отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других информационных системах).

Понятие ИС очень широкое и оно охватывает следующие системы:

- ЭВМ всех классов и назначений;

- вычислительные комплексы и системы;

- вычислительные сети (локальные, региональные и глобальные).

Такой широкий диапазон систем объединяется одним понятием по двум причинам: во-первых, для всех этих систем основные проблемы защиты информации являются общими; во-вторых, более мелкие системы являются элементами более крупных систем.

Если защита информации в каких-либо системах имеет свои особенности, то они рассматриваются отдельно.

**Предметом защиты** в ИС является информация. Материальной основой существования информации в ИС являются электронные и электромеханические устройства (подсистемы), а также машинные носители. С помощью устройств ввода или систем передачи данных (СПД) информация попадает в ИС. В системе информация хранится в запоминающих устройствах (ЗУ) различных уровней, преобразуется (обрабатывается) процессорами (ПЦ) и выводится из системы с помощью устройств вывода или СПД. В качестве машинных носителей используются магнитные ленты, диски различных типов, флеш-накопители. Ранее в качестве машинных носителей информации использовались бумажные перфокарты и перфоленты, магнитные барабаны и карты. Большинство типов машинных носителей информации являются съемными, т.е. могут сниматься с устройств и использоваться или храниться (ленты, диски, флеш) отдельно от устройств.

Таким образом, для защиты информации (обеспечения безопасности информации) в ИС необходимо защищать устройства (подсистемы) и машинные носители от несанкционированных (неразрешенных) воздействий на них.

Однако такое рассмотрение ИС с точки зрения защиты информации является неполным. Компьютерные системы относятся к классу человеко-машинных систем. Такие системы эксплуатируются специалистами (обслуживающим персоналом) в интересах пользователей. Причем, в последние годы пользователи имеют самый непосредственный доступ к системе. В некоторых ИС (например, ПЭВМ) пользователи выполняют функции обслуживающего персонала. Обслуживающий персонал и пользователи являются также носителями информации. Поэтому от несанкционированных воздействий необходимо защищать не только устройства и носители, но также обслуживающий персонал и пользователей.

Таким образом, более полное определение ИС будет таковым:

**Информационная система** взаимосвязанная совокупность средств, методов и персонала, которые используются для хранения, обработки, передачи и получения информации в интересах достижения поставленной цели. При решении проблемы защиты информации в ИС необходимо учитывать также противоречивость человеческого фактора системы. Обслуживающий персонал и пользователи могут быть как объектом, так и источником несанкционированного воздействия на информацию.

Понятие "**объект защиты**" или "**объект**" чаще трактуется в более широком смысле. Для сосредоточенных ИС или элементов распределенных систем понятие "объект" включает в себя не только информационные ресурсы, аппаратные, программные средства, обслуживающий персонал, пользователей, но и помещения, здания, и даже прилегающую к зданиям территорию.

Одними из основных понятий теории защиты информации являются понятия "безопасность информации" и "защищенные ИС".

**Безопасность (защищенность) информации в ИС** – это такое состояние всех компонент информационной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне. ИС, в которых обеспечивается безопасность информации, называются **защищенными**.

Безопасность информации в ИС (информационная безопасность) является одним из основных направлений обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной фирмы.

Информационная безопасность достигается проведением руководством соответствующего уровня **политики информационной безопасности**. Одноименный документ разрабатывается и принимается как официальный руководящий документ, ведомством, организацией. В документе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации в ИС. В программах информационной безопасности содержатся также общие требования и принципы построения систем защиты информации в ИС.

Под **системой защиты информации в ИС** понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в ИС в соответствии с принятой политикой безопасности.

Правильный подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и **интересов** этих субъектов, связанных с использованием информационных систем (ИС). Из этого положения можно вывести два важных следствия:

1. Трактовка понятия «информационная безопасность», для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае «пусть лучше все сломается, чем враг узнает хоть один секретный бит», во втором «да нет у нас никаких секретов, лишь бы все работало».

Зачем надо защищаться? Ответов на этот вопрос может быть множество, в зависимости от структуры и целей предприятия. Для одних первой задачей является предотвращение утечки информации (маркетинговых планов, перспективных разработок и т.д.) конкурентам. Другие могут пренебречь конфиденциальностью своей информации и сосредоточить внимание на ее целостности. Например, для банка важно в первую очередь обеспечить неизменность обрабатываемых платежных поручений, чтобы злоумышленник не смог несанкционированно дописать в платежку еще один нолик или изменить реквизиты получателя. Для третьих на первое место поднимается задача обеспечения доступности и безотказной работы информационных систем. Для провайдера *Internet*-услуг, компании, имеющей *Web*-сервер, или оператора связи первейшей задачей является именно обеспечение безотказной работы всех (или наиболее важных) узлов своей информационной системы. Расставить такого рода приоритеты можно только по результатам анализа деятельности предприятия.

2. Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от **поломки системы, вызвавшей перерыв в работе**. Более того, для многих открытых организаций (например, учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте. Главное для них это обеспечение непрерывности работы информационной системы.

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от **поддерживающей инфраструктуры**, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Эта инфраструктура имеет самостоятельную ценность, но нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций.

Обратим внимание, что в определении ИБ перед существительным «**ущерб**» стоит прилагательное «**неприемлемый**». Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а *целью защиты информации становится уменьшение размеров ущерба до допустимых значений*.

***1.3 Основные составляющие информационной безопасности***

Информационная безопасность – многогранная область деятельности, в которой успех может принести только систематический, комплексный подход.

**Цель информационной безопасности** обеспечить бесперебойную работу организации и свести к минимуму ущерб от событий, таящих угрозу безопасности, посредством их предотвращения и сведения последствий к минимуму.

Основными задачами и составляющими ИБ является: обеспечение **доступности**, **целостности** и **конфиденциальности** информационных ресурсов и поддерживающей инфраструктуры.

Поясним понятия доступности, целостности и конфиденциальности.

**Доступность** – это возможность за приемлемое время получить требуемую информационную услугу.

Под **целостностью** информации подразумевается, ее защищенность от разрушения и несанкционированного изменения.

Наконец, **конфиденциальность** – это защита от несанкционированного доступа к информации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент информационной безопасности.

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

**Целостность** можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит «руководством к действию». Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Неприятно и искажение официальной информации, будь то текст закона или страница ВЭБ-сервера какой-либо правительственной организации.

**Конфиденциальность** – самый проработанный у нас в стране аспект информационной безопасности. Обеспечение конфиденциальности достигается использованием криптографии и выполнением соответствующих организационных и технических мероприятий направленных на выявление и блокирование возможных каналов утечки информации.

Почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность – какой смысл в информационной услуге, если она содержит искаженные сведения?

Наконец, конфиденциальные моменты есть также у многих организаций (даже в упоминавшихся выше учебных институтах стараются не разглашать сведения о зарплате сотрудников) и отдельных пользователей (например, пароли).

***1.4 Управление информационной безопасностью***

Обеспечение ИБ это непрерывный процесс, основное содержание которого составляет управление. ИБ невозможно обеспечить разовым мероприятием, поскольку средства защиты нуждаются в постоянном контроле и обновлении.

**Управление информационной безопасностью** это управление людьми, рисками, ресурсами, средствами защиты и т.п. УИБ является неотъемлемым элементом управления предприятием и позволяет коллективно использовать конфиденциальную информацию, обеспечивая при этом ее защиту, а так же защиту вычислительных ресурсов.

**Управление информационной безопасностью** - это циклический процесс, включающий:

- осознание степени необходимости защиты информации;

- сбор и анализ данных о состоянии информационной безопасности в организации;

- оценку информационных рисков;

- планирование мер по обработке рисков;

- реализацию и внедрение соответствующих механизмов контроля;

- распределение ролей и ответственности;

- обучение и мотивацию персонала;

- оперативную работу по осуществлению защитных мероприятий;

- мониторинг функционирования механизмов контроля,

- оценку их эффективности и соответствующие корректирующие воздействия.

Для обеспечения необходимого уровня информационной безопасности (предприятия, учреждения и т.д.) на предприятии создается комплексная **система управления информационной безопасностью** (**СУИБ**). Конечной целью создания такой системы является предотвращение или минимизация ущерба (прямого или косвенного, материального, морального или иного), преднамеренно наносимого злоумышленниками либо непреднамеренно - нерадивыми работниками предприятия посредством нежелательного воздействия на информацию, ее носители и процессы обработки.

Согласно стандарту *ISO* 27001, **система управления информационной безопасностью** (СУИБ) – это «та часть общей системы управления организации, основанной на оценке бизнес рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности». Система управления включает в себя организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы.

**Основной задачей** системы является обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов (ресурсов) ИС.

***Какие преимущества компании дает внедрение СУИБ и ее сертификация на соответствие международным стандартам***:

- повышение управляемости и надежности бизнеса компании;

- повышение защищенности ключевых бизнес-процессов компании;

- повышение доверия к компании как к партнеру, так и клиенту;

- соответствие компании требованиям международного стандарта подчеркивает чистоту и прозрачность бизнеса компании;

- наличие СУИБ и международного сертификата упрощает процедуру выхода компании на внешние рынки;

- международное признание и повышение авторитета компании как на внутреннем, так и внешнем рынках;

- повышение доходности бизнеса в целом.

***Для структурных подразделений компании внедрение СУИБ и ее сертификация на соответствие международным стандартам дает следующие преимущества***:

- Систематизация процессов обеспечения информационной безопасности;

- Расстановка приоритетов компании в сфере ИБ;

- Управление ИБ компании в рамках единой корпоративной политики;

- Своевременное выявление и управление рисками;

- Снижение рисков от внутренних и внешних угроз;

- Оптимизация управленческих процессов;

- Повышение эффективности функционирования СУИБ и защищенности информационных систем;

- Повышение общей корпоративной культуры сотрудников и вывод управления бизнесом на новый уровень.

***1.5 Важность и сложность проблемы информационной безопасности***

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю - национальном, отраслевом, корпоративном или персональном.

Для иллюстрации этого положения ограничимся несколькими примерами. В Доктрине информационной безопасности Украины отмечено, что информационная безопасность является неотъемлемой составляющей каждой из сфер национальной безопасности. В то же время информационная безопасность является важной самостоятельной сферой обеспечения национальной безопасности. Именно поэтому развитие Украины как суверенного, демократического, правового и экономически стабильного государства возможно только при условии обеспечения надлежащего уровня ее информационной безопасности.

Американский ракетный крейсер «Йорктаун» был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением (июль 1998). Таким оказался побочный эффект программы ВМФ США по максимально широкому использованию коммерческого программного обеспечения с целью снижения стоимости военной техники.

Заместитель начальника управления по экономическим преступлениям Министерства внутренних дел России сообщил, что российские хакеры с 1994 по 1996 год предприняли почти 500 попыток проникновения в компьютерную сеть Центрального банка России. В 1995 году ими было похищено 250 миллиардов рублей (ИТАР-ТАСС, АР, 17 сентября 1996 года). Как сообщил журнал "Internet week" от 23 марта 1998 года, потери крупнейших компаний, вызванные компьютерными вторжениями, продолжают увеличиваться, несмотря на рост затрат на средства обеспечения безопасности. Согласно результатам совместного исследования Института информационной безопасности и ФБР, в 1997 году ущерб от компьютерных преступлений достиг 136 миллионов долларов, что на 36% больше, чем в 1996 году. Каждое компьютерное преступление наносит ущерб примерно в 200 тысяч долларов.

В феврале 2001 года двое бывших сотрудников одной из компаний, воспользовавшись паролем администратора, удалили с сервера файлы, составлявшие крупный (на несколько миллионов долларов) проект для иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери ограничились расходами на следствие и средства защиты от подобных инцидентов в будущем. В августе 2002 года преступники предстали перед судом.

Одна студентка потеряла стипендию в 18 тысяч долларов в Мичиганском университете из-за того, что ее соседка по комнате воспользовалась их общим системным входом и отправила от имени своей жертвы электронное письмо с отказом от стипендии.

Понятно, что подобных примеров множество, можно вспомнить и другие случаи - недостатка в нарушениях ИБ нет и не предвидится.

Приведем еще несколько цифр. В марте 1999 года был опубликован очередной, четвертый по счету, годовой отчет «Компьютерная преступность и безопасность-1999: проблемы и тенденции». В отчете отмечается резкий рост числа обращений в правоохранительные органы по поводу компьютерных преступлений (32% из числа опрошенных); 30% респондентов сообщили о том, что их информационные системы были взломаны внешними злоумышленниками; атакам через Интернет подвергались 57% опрошенных; в 55% случаях отмечались нарушения со стороны собственных сотрудников. Примечательно, что 33% респондентов на вопрос «были ли взломаны ваши ВЭБ-серверы и системы электронной коммерции за последние 12 месяцев?» ответили «не знаю».

В аналогичном отчете, опубликованном в апреле 2002 года, цифры изменились, но тенденция осталась прежней: 90% респондентов (преимущественно из крупных компаний и правительственных структур) сообщили, что за последние 12 месяцев в их организациях имели место нарушения информационной безопасности; 80% констатировали финансовые потери от этих нарушений; 44% (223 респондента) смогли и/или захотели оценить потери количественно, общая сумма составила более 455 млн. долларов. Наибольший ущерб нанесли кражи и подлоги (более 170 и 115 млн. долларов соответственно).

Столь же тревожные результаты содержатся в обзоре Information week, опубликованном 12 июля 1999 года. Лишь 22% респондентов заявили об отсутствии нарушений информационной безопасности. Наряду с распространением вирусов отмечается резкий рост числа внешних атак.

Увеличение числа атак еще не самая большая неприятность. Хуже то, что постоянно обнаруживаются новые уязвимые места в программном обеспечении (выше мы указывали на ограниченность современной технологии программирования) и, как следствие, появляются новые виды атак.

Так, в информационном письме Национального центра защиты инфраструктуры США от 21 июля 1999 года сообщается, что за период с 3 по 16 июля 1999 года выявлено девять проблем с ПО, риск использования которых оценивается как средний или высокий (общее число обнаруженных уязвимых мест равно 17). Среди «пострадавших» операционных платформ почти все разновидности ОС Unix, Windows, МаcОС, так что никто не может чувствовать себя спокойно, поскольку новые ошибки тут же начинают активно использоваться злоумышленниками.

В таких условиях системы информационной безопасности должны уметь противостоять разнообразным атакам, как внешним, так и внутренним, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды; порой прощупывание уязвимых мест ведется медленно и растягивается на часы, так что подозрительная активность практически незаметна. Целью злоумышленников может быть нарушение всех составляющих ИБ - доступности, целостности или конфиденциальности.