Угрозы информации

Вводная часть

В ходе данного занятия рассмотрим понятия «угроза информации» и рассмотрим классификацию данной категории.

Актуальность данного занятия определяется тем, что с помощью современных программ, а также компьютерных технологий, люди достигли больших высот и преобразований почти во всех сферах жизни общества. Однако, эти достижения имеют свои уязвимые аспекты: во-первых, человек стал зависим от своих технологий, во-вторых, теперь уязвимость одной технологии может привести к потере любой защищаемой информации и, как следствие, банкротству организации, обладавшей данной информацией. Кроме этого, есть те, кто желает воспользоваться конфиденциальной информацией в корыстных целях.

Организации, а также их информационные системы и сети сталкиваются с угрозами безопасности из широкого диапазона источников, включая компьютерное мошенничество, шпионаж, саботаж, вандализм, пожар или наводнение. Источники ущерба, например, вредоносный код, компьютерное хакерство и атаки типа отказа в обслуживании, становятся более распространенными и все более и более изощренными.

В настоящее время в Российской Федерации существует несколько концепций разработки систем защиты информации. Их конкретное применение во многом определяется требованиями государственных стандартов и нормативных документов Федеральной службы по техническому и экспортному контролю (ФСТЭК) и ФСБ, регулирующих деятельность по управлению защитой информации в АСУ и информационных системах различного назначения.

Принципиально можно выделить два подхода к созданию системы защиты информации.

Первый из них относится к построению систем защиты информации в информационных системах организаций, ИС персональных данных, объектах с критической информационной инфраструктурой, банковской тайны и относится к гарантированной защите информации. Методика создания системы защиты информации основана на анализе угроз информационной безопасности для конкретного объекта защиты, определения класса или уровня защиты информации в информационных системах и последующим внедрением регламентированных требований по защите информации для определенного класса (уровня) защиты информации.

Второй подход к созданию систем защиты информации основан на оценке показателей риска информационной безопасности для каждой выявленной угрозы по отношению к конкретному информационному активу через имеющиеся уязвимости информационной системы. Такой механизм защиты представляет особый интерес для разработчиков систем защиты информации в бизнесе, но вопросы оценки риска возникновения угрозы информации мы рассмотрим на следующих занятиях.

В ходе занятия будут рассмотрены следующие учебные вопросы:

1. Угрозы информации.
2. Классификация угроз информации.

Первый учебный вопрос: «Угрозы информации»

Специфика бизнеса, человеческий фактор, несовершенство законодательства и технические недостатки современных информационных систем обуславливают повышенный риск корпоративных информационных систем. К основным нарушениям защиты информации и информационной безопасности в целом, приносящим материальный ущерб, относятся: коммерческий шпионаж, утечки и потери информации из-за халатности сотрудников, внутренние инциденты с персоналом, компьютерные вирусы, хакеры и другие.

Угрозы безопасности, которые могут быть реализованы, например, с помощью скрытых каналов, включают в себя:

- внедрение вредоносных программ и данных;
- подачу злоумышленником команд агенту для выполнения;
- утечку криптографических ключей или паролей;
- утечку отдельных информационных объектов.

Для дальнейшего изучения угроз безопасности информации вы должны знать ряд понятий, определенных в **ГОСТ Р 53114-2008** «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

Угроза – совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности.

Угроза информационной безопасности организации – совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации.

Формой реализации или проявления угрозы ИБ является наступление одного или нескольких взаимосвязанных событий ИБ и инцидентов ИБ, приводящего(их) к нарушению свойств информационной безопасности объекта или объектов защиты организации.

Ущерб – отрицательные последствия, возникающие вследствие причинения вреда активам организации.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

В ходе занятий мы уже несколько раз встречаемся с терминами «конфиденциальность», «доступность» и «целостность», и в дальнейшем не

раз будем к ним обращаться. Термин «конфиденциальность информации» мы рассмотрели на предыдущем занятии. Поэтому напомню его формулировку и рассмотрим содержание категорий «доступность» и «целостность».

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (**ГОСТ Р 50922** «Защита информации. Основные термины и определения»).

Доступность информации (ресурсов информационной системы) – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Возвращаясь к **ГОСТ Р 53114** «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения», вы должны изучить следующие понятия:

Уязвимость – внутренние свойства объекта, создающие восприимчивость к воздействию источника риска, которое может привести к какому-либо последствию.

Атака – попытка преодоления системы защиты информационной системы.

Степень «успеха» атаки зависит от уязвимости и эффективности системы защиты.

Сетевая атака – действия с применением программных и (или) технических средств и с использованием сетевого протокола, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной информационной системы.

Сетевой протокол – совокупность семантических и синтаксических правил, определяющих взаимодействие программ управления сетью, находящейся на одном компьютере, с одноименными программами, находящимися на другом компьютере.

Угрозы и ущерб связаны между собой. Угрозы становятся возможными по причине уязвимостей в информационной системе.

Угроза может причинить ущерб активам организации, таким как информация, процессы и системы. Угрозы могут возникать в результате природных явлений или действий людей, они могут быть случайными или умышленными.

Должны быть установлены и случайные, и преднамеренные источники угроз. Угрозы могут проистекать как из самой организации, так и из источника вне ее пределов. Угрозы должны определяться в общем и по виду (например, неавторизованные действия, физический ущерб, технические сбои), а затем, где это уместно, отдельные угрозы определяются внутри родового класса. Это означает, что ни одна угроза, включая неожиданные угрозы, не будет упущена, но объем требуемой работы, несмотря на это,

сокращается. Некоторые угрозы могут влиять более чем на один актив. В таких случаях они могут быть причиной различных влияний в зависимости от того, на какие активы оказывается воздействие.

Для определения и количественной оценки вероятности возникновения угроз данные могут быть получены от владельцев активов или пользователей, персонала отдела кадров, руководства организации и специалистов в области ИБ, экспертов в области физической безопасности, специалистов юридического отдела и других структур, а также от юридических организаций, метеорологических служб, страховых компаний, национальных правительственных учреждений. При анализе угроз должны учитываться аспекты среды и культуры. Опыт, извлеченный из инцидентов, и предыдущие оценки угроз должны быть учтены в текущей оценке. При необходимости для заполнения перечня общих угроз может быть целесообразным справиться в других реестрах угроз (возможно, специфичных для конкретной организации или бизнеса). Списки угроз и их статистику можно получить от промышленных предприятий, федерального правительства, юридических организаций, страховых компаний и т.д. Используя списки угроз или результаты предыдущих оценок угроз, не следует забывать о том, что происходит постоянная смена значимых угроз, особенно, если изменяются бизнес-среда или информационные системы.

Угроза характеризуется наличием объекта угрозы, источника угрозы и проявления угрозы информационной безопасности.

Рассмотрим содержание объекта угрозы информационной безопасности.

Данная категория определяется методическим документом «Методика оценки угроз безопасности информации» (*утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.*).

В ходе оценки угроз безопасности информации должны быть определены информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям - объекты воздействия.

Совокупность объектов воздействия и их интерфейсов определяет границы процесса оценки угроз безопасности информации и разработки модели угроз безопасности информации.

Исходными данными для определения возможных **объектов угрозы являются**:

а) общий перечень угроз безопасности информации, содержащейся в банке данных угроз безопасности информации ФСТЭК России, модели угроз безопасности информации, разрабатываемые ФСТЭК России;

б) описания векторов компьютерных атак, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

в) документация на сети и системы (в части сведений о составе и архитектуре, о группах пользователей и уровне их полномочий, и типах доступа, внешних и внутренних интерфейсах);

г) договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (в случае функционирования систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры);

д) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой.

Указанные исходные данные могут быть дополнены иными документами и сведениями с учетом особенностей области деятельности, в которой функционируют системы и сети.

Объекты воздействия и виды воздействия на них должны быть конкретизированы применительно к архитектуре и условиям функционирования систем и сетей, а также областям и особенностям деятельности обладателя информации и оператора.

Товарищи студенты! Мы рассмотрели, что исходными данными для определения возможных объектов воздействия являются, в том числе общий перечень угроз безопасности информации, содержащейся в банке данных угроз безопасности информации ФСТЭК России, модели угроз безопасности информации, разрабатываемые ФСТЭК России.

Что представляет собой ***Банк данных угроз безопасности информации*** и ***модель угроз***?

Целью создания и ведения настоящего Банка данных угроз безопасности информации является повышение информированности заинтересованных лиц о существующих угрозах безопасности информации в информационных (автоматизированных) системах.

Банк данных угроз безопасности информации предназначен для заказчиков, операторов, разработчиков информационных (автоматизированных) систем и их систем защиты, разработчиков и производителей средств защиты информации, испытательных лабораторий и органов по сертификации средств защиты информации, а также иных заинтересованных организаций и лиц.

Банк данных угроз безопасности информации содержит сведения об основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов.

Сведения об угрозах безопасности информации и уязвимостях программного обеспечения, содержащиеся в Банке данных угроз безопасности информации, не являются исчерпывающими и могут быть дополнены по результатам анализа угроз безопасности информации и

уязвимостей в конкретной информационной (автоматизированной) системе с учетом особенностей ее эксплуатации (рис.1).

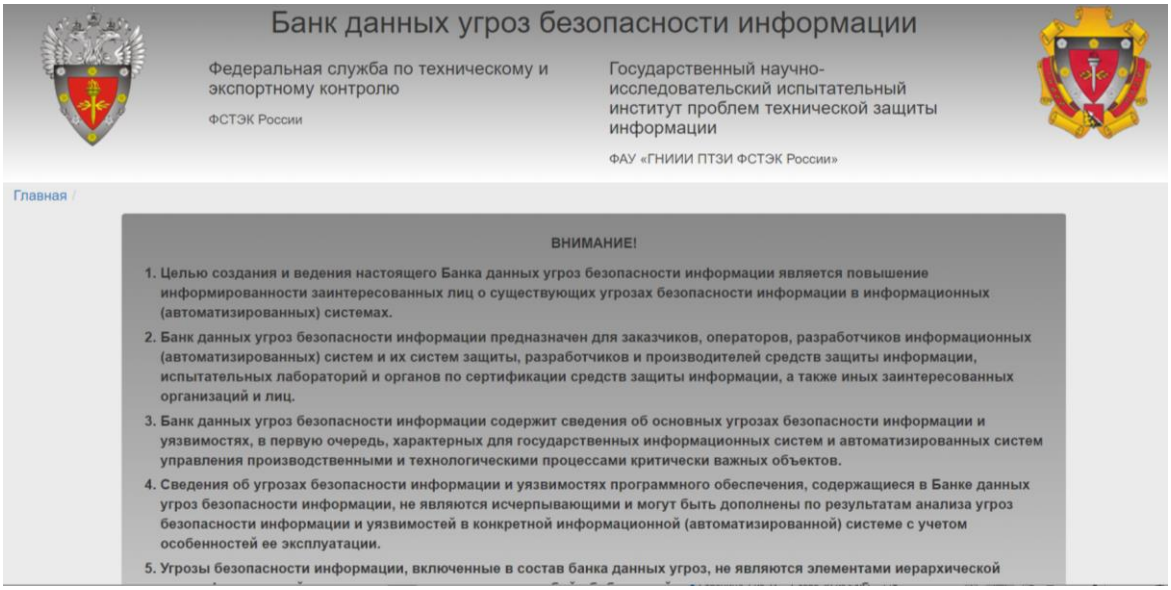

Рисунок – 1 Банк данных угроз безопасности информации

При определении угроз безопасности информации учитываются структурно-функциональные характеристики системы защиты информации, включающие наличие элементов автоматизированной системы управления, физические, логические, функциональные и технологические взаимосвязи в системе защиты информации, в том числе взаимодействие автоматизированной системы управления с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями, режимы функционирования системы защиты информации, а также иные особенности ее построения и функционирования.

По результатам определения угроз безопасности информации могут разрабатываться рекомендации по корректировке структурно-функциональных характеристик системы защиты информации, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Банк данных угроз безопасности информации постоянно обновляется (рис. 2).

Визуально Банк данных угроз безопасности информации содержит следующие данные:

1. Общие сведения об угрозе безопасности информации:
- идентификатор угрозы безопасности информации;
- наименование угрозы безопасности информации;
- описание угрозы безопасности информации;
- источник угрозы (характеристика и потенциал нарушителя);
- объект воздействия угрозы безопасности информации;

2. Последствия воздействия угрозы безопасности информации

- нарушение конфиденциальности (1 или 0);
- нарушение целостности (1 или 0);
- нарушение доступности (1 или 0);

3. Дополнительные сведения об угрозы безопасности информации:
- дата включения угрозы в банк угроз безопасности информации;
- дата последнего изменения данных.

Аналогично можно получить сведения по уязвимостям.

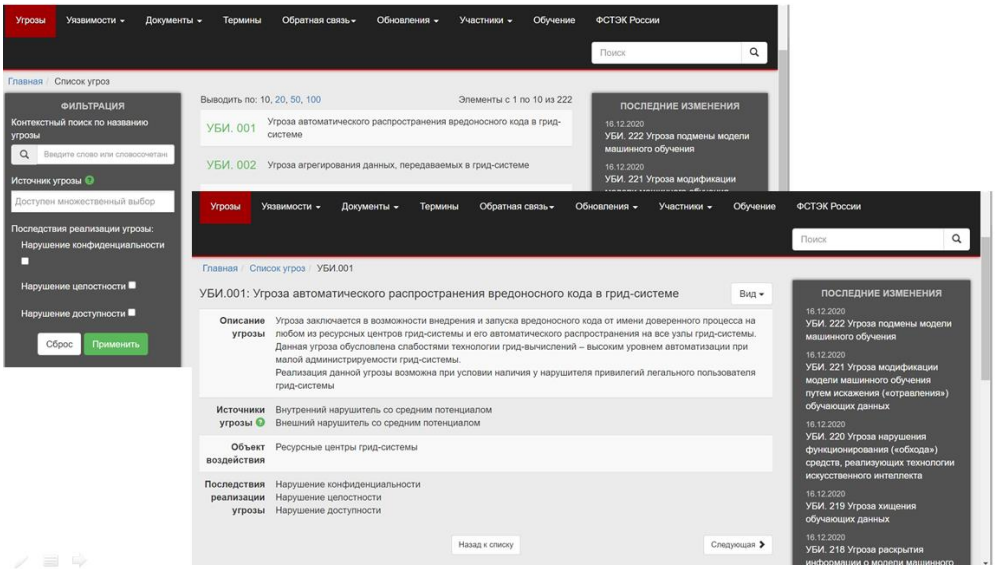

Рисунок – 2 Структура банка данных угроз безопасности информации

Следующей элемент, являющийся исходными данными для определения возможных объектов воздействия – это ***модель угроз безопасности информации***. Она должна содержать описание системы защиты информации и угроз безопасности информации для каждого из уровней системы защиты информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей автоматизированной системы управления, способов (сценариев) реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (доступности, целостности, конфиденциальности) и штатного режима функционирования системы защиты информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы ФСТЭК России.

Порядок моделирования угроз безопасности представлен на рисунке 3 в виде схемы.

Данный порядок включает в себя пять этапов, выполняемых в определенной последовательности. Общая схема процесса, представленная в Методике, выглядит следующим образом.

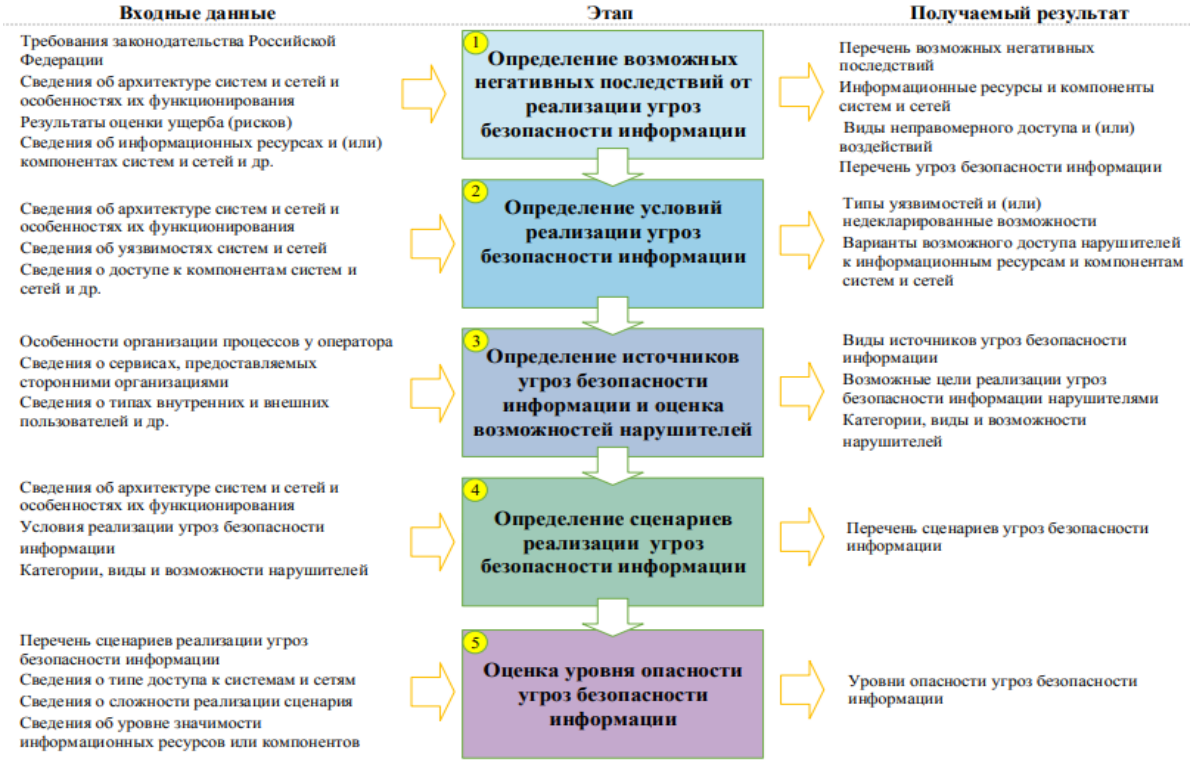

Рисунок 3 – Порядок моделирования угроз безопасности

За ***определение актуальности угрозы безопасности информации*** отвечают этапы с первого по четвертый. В соответствии с Методикой, угроза безопасности будет являться актуальной при наличии хотя бы одного сценария ее реализации и, если ее реализация приведет к каким-либо негативным последствиям для обладателя информации (оператора) или государства.

Цель пятого этапа – ***определить опасность каждой из актуальных угроз***. По сути, ***данная характеристика носит исключительно информационный характер*** и не оказывает прямого влияния ни на итоговый документ, формируемый по результатам моделирования, ни на возможные варианты нейтрализации угрозы. Можно предположить, что данный параметр должен использоваться для определения очередности закрытия угрозы, однако малое число возможных значений показателя – «низкий», «средний», «высокий» – не позволяют сделать это с достаточной степенью детализации. Более того, любая из дошедших до данного шага угроз должна быть так или иначе закрыта, поэтому забыть про «неопасную» угрозу попросту не получится. Таким образом, истинная цель данного параметра остается не раскрытой в полной мере.

Стоит отметить, что работы по моделированию угроз безопасности должны проводиться либо обладателем информации (оператором) самостоятельно, либо с привлечением лицензиатов ФСТЭК.

Подробнее рассмотрим ***порядок определения актуальности угроз безопасности***.

На ***первом этапе*** предлагается определить ***все возможные негативные последствия от реализации угроз безопасности***. Помогать в этом должна либо проведенная ранее оценка ущерба (рисков) от нарушения основных критических процессов, либо экспертная оценка, либо информация, получаемая от эксплуатирующих информационную систему подразделений.

При любом выбранном подходе, необходимо определить информационные ресурсы, обеспечивающие выполнение критических процессов (непосредственно информация, программно-аппаратные средства, средства защиты информации и иные) и основные виды неправомерного доступа по отношению к каждому из ресурсов. Методичка содержит перечень основных видов ресурсов и неправомерного доступа к ним, а также примеры определения возможных негативных последствий.

2. На ***втором этапе*** необходимо определить наличие ***потенциальных уязвимостей и их типы, наличие недекларированных возможностей в информационных системах, а также необходимость доступа к системе для реализации каждой из угроз безопасности***.

В качестве основного метода выявления потенциальных уязвимостей в информационной системе на этапе ее эксплуатации является тестирование на проникновение, проводимое в том числе с учетом функциональных возможностей и настроек средств защиты.

3. Следующим, ***третьим этапом*** является ***определение нарушителей безопасности***, как **источника угроз информационной безопасности** и оценка их возможностей. В качестве источников угроз предлагается рассматривать как антропогенные, так и техногенные: первые рассматриваются абсолютно для всех информационных систем, тогда как вторые – только для тех систем, для которых предъявляются требования к устойчивости и надежности функционирования.

Подход к определению возможных ***антропогенных источников угроз – нарушителей*** – является стандартным и заключается в выявлении конкретных видов нарушителей, их потенциала и возможностей при реализации угроз в отношении защищаемой информационной системы. Стоит отметить, что при наличии связи информационной системы с Интернетом, внешний нарушитель как минимум с низким потенциалом всегда рассматривается в качестве актуального источника угроз.

Необходимо обратить внимание, что согласно Методике, нарушитель может обладать одним из четырех уровней потенциала (базовый, базовый повышенный, средний и высокий).

На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации определяются виды нарушителей, актуальных для систем и сетей.

Основными **видами нарушителей**, подлежащих оценке, являются:

- специальные службы иностранных государств;
- террористические, экстремистские группировки;

- преступные группы (криминальные структуры);
- отдельные физические лица (хакеры);
- конкурирующие организации;
- разработчики программных, программно-аппаратных средств;
- лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
- поставщики услуг связи, вычислительных услуг;
- лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
- лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);
- авторизованные пользователи систем и сетей;
- системные администраторы и администраторы безопасности;
- бывшие (уволенные) работники (пользователи).

Указанные виды нарушителей могут быть дополнены иными нарушителями с учетом особенностей области деятельности, в которой функционируют системы и сети. Для одной системы и сети актуальными могут являться нарушители нескольких видов.

Нарушители признаются актуальными для систем и сетей, когда возможные цели реализации ими угроз безопасности информации могут привести к определенным для систем и сетей негативным последствиям и соответствующим рискам (видам ущерба).

Возвращаемся к схеме модели угроз, показанной выше на рис. 3.

4. На четвертом этапе осуществляется **анализ возможных тактик и техник реализации угроз.** Для определения возможных сценариев атак, Методика предлагает использовать приведенные в ней тактики и техники, а также дополнительную информацию из БДУ ФСТЭК или иных баз данных компьютерных атак (здесь имеются в виду матрица ATT&CK и аналогичные походы).

Сценарии реализации угроз безопасности информации должны быть определены для соответствующих способов реализации угроз безопасности информации, определенных в соответствии с настоящей Методикой, и применительно к объектам воздействия и видам воздействия на них. Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

На этапе создания систем и сетей должен быть определен хотя бы один сценарий каждого способа реализации возможной угрозы безопасности информации. Сценарий определяется для каждого актуального нарушителя и их уровней возможностей.

При наличии хотя бы одного сценария угрозы безопасности информации такая угроза признается актуальной для системы и сети и

включается в модель угроз безопасности систем и сетей для обоснования выбора организационных и технических мер по защите информации (обеспечению безопасности), а также выбора средств защиты информации.

На этапе эксплуатации систем и сетей для каждой возможной угрозы безопасности информации определяется множество возможных сценариев ее реализации в интересах оценки эффективности принятых технических мер по защите информации (обеспечению безопасности), в том числе средств защиты информации. При этом множество сценариев определяется для каждого актуального нарушителя и уровней его возможностей в соответствии с полученными результатами инвентаризации систем и сетей, анализа уязвимостей и (или) тестирования на проникновение, проведенных с использованием автоматизированных средств.

На этапе эксплуатации определение сценариев реализации угрозы включает:

а) анализ исходных данных на систему или сеть, предусматривающий в том числе анализ документации, модели угроз безопасности информации, применяемых средств защиты информации, и определение планируемых к применению автоматизированных средств;

б) проведение инвентаризации информационных систем и сетей и определение объектов воздействия и их интерфейсов;

в) определение внешних интерфейсов, которые могут быть задействованы при реализации угроз безопасности информации;

г) определение внутренних интерфейсов, которые могут быть задействованы при реализации угроз безопасности информации;

д) выявление уязвимостей объектов воздействия, а также компонентов систем и сетей, имеющих внешние интерфейсы, с которыми посредством внутренних интерфейсов взаимодействуют объекты воздействия;

е) проведение тестирования на проникновение, подтверждающего возможность использования выявленных уязвимостей или выявления новых сценариев реализации угрозы безопасности информации;

ж) поиск последовательности тактик и техник, применение которых может привести к реализации угрозы безопасности информации, исходя из уровня возможностей актуальных нарушителей, а также результатов инвентаризации, анализа уязвимостей и тестирования на проникновение;

з) составление сценариев реализации угрозы безопасности информации применительно к объектам и видам воздействия, а также способам реализации угроз безопасности информации.

На этом изложение первого учебного вопроса завершено.

Второй учебный вопрос: «Классификация угроз информационной безопасности»

Угрозы чрезвычайно разнообразны, поэтому мы рассмотрим их общую классификацию. В частности, угрозы можно классифицировать по их носителям, по целям, по причиненному ущербу, по наличию умысла, по степени подготовленности и профессионализму нарушителей, по скрытности исполнения, по удаленности от объекта защиты и еще множеству различных признаков.

Классификацию угроз информационной безопасности можно разделить на четыре большие группы:

1. ***По аспекту ИБ***: угрозы конфиденциальности, угрозы целостности, угрозы доступности.

2. ***По сфере воздействия на информационную систему***: внутри или вне рассматриваемой АИС; угрозы, возникновение которых обусловлено человеческим фактором. Угрозы со стороны инсайдеров (лиц, имеющих доступ к скрытой и достоверной информации) являются наиболее опасными.

3. ***По компонентам АИС, на которые нацелена угроза***: данные, программное обеспечение, аппаратное обеспечение, поддерживающая инфраструктура; угрозы, связанные с техническими и программными средствами, используемыми при разработке и эксплуатации информационных систем.

4. ***По природе возникновения***: естественные (объективные) и искусственные (субъективные); техногенные угрозы, возникающие вследствие форс-мажорных обстоятельств.

Рассмотрим данную классификацию угроз информационной безопасности.

Первая группа угроз – угрозы по аспекту ИБ. *угрозы конфиденциальности, угрозы целостности, угрозы доступности.*

Угрозы конфиденциальности реализуются, если защищаемая информация, обладающая действующей или потенциальной ценностью в силу ее неизвестности третьим лицам, становится достоянием этих лиц (одного или многих).

В некоторых случаях угрозу конфиденциальности может нести не только раскрытие содержания скрываемой информации, но ставший известным сам факт существования такой информации. Например, тайной может являться не только содержание международного договора или финансовой сделки, но и сам факт такого соглашения.

Угрозы целостности информации выражаются в ее несанкционированной или непреднамеренной модификации. Т.е. угрозы изменения ее содержания.

Правомерен вопрос: какое количество информации необходимо изменить, чтобы наступила угроза целостности? Это, безусловно, зависит от вида информации. Если защищаемая информация представляет собой текст,

запись голоса, музыкальное произведение, рисунок, то порча или искажение ее части могут не привести к потере качества.

Угроза целостности представляет опасность не только для данных. Модификация компьютерной программы, делающая возможной перехват управления компьютером с целью совершения шпионских или деструктивных действий, тоже является разновидностью угроз целостности. Нарушение целостности информации вредит двум ее прагматическим качествам – полноте и достоверности. Косвенным следствием угрозы целостности является утрата доверия к источнику или носителю информации.

Угрозы доступности выражаются в том, что защищаемая информация оказывается заблокированной, т. е. в течение некоторого времени недоступной для ее собственника, владельца или пользователя. При этом информация сохраняется в неизменном виде и не становится достоянием третьих лиц. Блокирование информации может произойти по какой-либо из перечисленных ниже причин:

- поломки ключа или замка от сейфа, в котором хранятся носители конфиденциальной информации;
- забывчивости пользователя, приводящей к утрате пароля для расшифровывания электронного документа;
- повреждения служебной области данных на магнитном или оптическом диске либо неисправности устройства считывания/записи данных (если поврежден участок носителя, где была записана защищаемая информация, следует говорить об угрозах целостности).

Угроза доступности реализуется и в том случае, если информация временно оказывается заблокированной для автоматизированной информационной системы. Например, страшные по своим возможным последствиям переключения на посторонние задачи компьютерных систем, управляющих ядерной реакцией или движением транспорта, тоже являются примерами угроз доступности информации.

Собственник, организующий защиту своей информации, должен ясно представлять себе характер потенциальных угроз и четко осознавать, что с помощью одного и того же набора средств и методов защитить информацию от всех трех типов угроз невозможно.

Вторая группа угроз – угрозы по сфере воздействия на информационную систему.

Внутри или вне рассматриваемой АИС; угрозы, возникновение которых обусловлено человеческим фактором. Угрозы со стороны инсайдеров (лиц, имеющих доступ к скрытой и достоверной информации) являются наиболее опасными.

Источники угроз ИБ можно разделить на внутренние и внешние.

К ***внутренним*** источникам угроз информационной безопасности относятся:

- внутренние нарушители информационной безопасности;

- аппаратные средства, используемые в информационной системе (рабочие станции, серверы, принтеры, внешнее оборудование, источники бесперебойного питания и другие);
- программные средства (системное и прикладное программное обеспечение);
- сетевое оборудование (маршрутизаторы, коммутаторы, модемы, каналы связи и т.д.);
- системы жизнеобеспечения (системы энергоснабжения, системы кондиционирования и водоснабжения).

К ***внешним*** источникам угроз информационной безопасности относятся:

- внешние нарушители информационной безопасности ИС;
- форс-мажорные обстоятельства.

По мотивации воздействия на информационные ресурсы и системы, источники угроз ИБ можно разделить на преднамеренные и случайные.

Преднамеренные (умышленные) угрозы связаны с корыстными стремлениями людей (злоумышленников).

Случайные (неумышленные) угрозы вызваны ошибками в проектировании элементов информационных систем, в программном обеспечении, в действиях сотрудников и т.п.

Угрозы, обусловленные человеческим фактором.

Данный класс угроз весьма обширен, к нему относятся угрозы, возникающие вследствие умышленных или неумышленных действий человека:

- *неправомерные действия авторизованных пользователей в системах и приложениях*, что выражается в использовании нарушителем учетной записи, к которой ему разрешен доступ, в неразрешенных целях, в том числе неправомерные действия в системах управления сетями телекоммуникаций, биллинговых, финансовых и технологических системах. Эти же угрозы могут исходить и от других категорий лиц: администраторов, временных и удалённых пользователей, программистов, партнёров;
- *отказ в обслуживании*, т.е. выполнение намеренных действий, направленных на возникновение отказа в обслуживании в системах, приложениях, базах и сетях передачи данных. Такой вид угроз может исходить от администраторов, технического персонала, внешних злоумышленников, программистов, партнёров; авторизованных, удалённых и временных пользователей;
- *внедрение вредоносного или разрушающего программного обеспечения*, включающего вирусы, «троянских коней», «червей», «логические бомбы» и приводящее к сбою или нарушению в работе компонентов информационных систем, а также получению полного контроля над уязвимой системой. К такому виду угроз могут быть причастны внешние злоумышленники; авторизованные, удалённые и временные пользователи,

партнёры (конкуренты), разработчики, программисты, технический персонал, администраторы;

- *подмена имени пользователя авторизованными пользователями*, выражающаяся в получении доступа (например, с помощью использования чужой учетной записи) авторизованными пользователями к информации, доступ к которой им запрещен. Данный вид угроз может исходить от авторизованных, удалённых и временных пользователей; технического персонала, партнёров (конкурентов) и администраторов;
- *подмена имени пользователя посторонними лицами*, выражающаяся в получении посторонними лицами доступа к информации под именем авторизованного пользователя. Основная угроза в этом случае может исходить от внешних злоумышленников и посетителей.
- *неправомерное использование системных ресурсов*, связанное с использованием аппаратного и программного обеспечения информационной системы в нерабочих целях, например, компьютерные игры, просмотр фильмов, использование доступа в Интернет в целях, не относящихся к выполнению функциональных обязанностей; использование ресурсов для несанкционированного выполнения работ для сторонних организаций и в личных целях. Эти угрозы могут исходить от авторизованных, удалённых и временных пользователей, технического персонала, программистов, администраторов;
- *ошибки в операциях*, выражающиеся в совершении ошибок сотрудниками организации при выполнении операций, связанных с эксплуатацией программно-аппаратных средств информационной системы. Данные угрозы могут исходить в основном от администраторов и партнёров организации;
- *ошибки в обслуживании аппаратного обеспечения*, т.е. компьютерной, множительной техники, сетевого оборудования и прочего в процессе технического обслуживания аппаратных средств техническим персоналом;
- *ошибки пользователя при работе с приложениями*. К данным угрозам могут быть причастны авторизованные, удалённые и временные пользователи, а также партнёры;
- *проникновение в корпоративную сеть*. Данная угроза может быть реализована одним из следующих способов:

- проникновение хакера в систему с использованием, например, атаки с переполнением буфера;
- проникновение в систему с подменой участника сетевого соединения;
- проникновение в систему с подменой IP-, MAC-адресов;
- осуществление атаки с заведомым введением в заблуждение и другие.

В любом случае, подобные угрозы исходят от внешних злоумышленников;

- *манипулирование информацией*. К данной угрозе относятся:

- подмена информации на веб-сайте организации, партнеров;

- рассылка заведомо ненужной адресату информации (бомбардирование спамом);
- внедрение ложных сообщений;
- намеренное нарушение очередности доставки информации;
- намеренная задержка доставки информации;
- намеренный сбой маршрутизации;
- перехват, изменение и перенаправление сообщения атакующей стороной посредством посылки сообщения через скомпрометированную рабочую станцию или компьютер злоумышленника.

Эти виды угроз исходят от внешних злоумышленников, администраторов, технического персонала, авторизованных, удалённых и временных пользователей, партнёров (конкурентов), программистов;

- *перехват информации*. К данной угрозе относятся:
- пассивный перехват информации;
- активный перехват информации;
- несанкционированный мониторинг трафика.

Эти виды угроз исходят от авторизованных, удалённых и временных пользователей; технический персонал, внешние злоумышленники, программисты, партнёры (конкуренты) и администраторы;

- *отрицание приема/передачи сообщений*. К данной угрозе относятся следующие случаи:
- пользователи сети отрицают, что они посылали сообщение (отрицание передачи);
- пользователи сети отрицают, что они приняли сообщение (отрицание приема).

К данным угрозам могут быть причастны авторизованные, удалённые и временные пользователи, технический персонал, программисты, администраторы и партнёры;

- *кражи персоналом документов, а также имущества, находящихся в помещениях организации*. К этому могут быть причастны обслуживающий и технический персонал, пользователи, программисты, администраторы;
- *кражи посторонними лицами* документов, а также имущества, в том числе, осуществившими незаконное проникновение в помещения организации. Данный вид угроз исходит от посетителей и временных пользователей;
- *умышленная порча имущества сотрудниками организации* путем совершения актов вандализма и причинения физического ущерба техническим средствам, носителям информации, системам жизнеобеспечения. Такие угрозы могут исходить от обслуживающего и технического персонала, пользователей, программистов и администраторов;
- *умышленная порча имущества посторонними лицами, не являющимися сотрудниками организации*, в том числе, осуществившими незаконное проникновение на объекты организации. Эти угрозы могут исходить от посетителей и временных пользователей.

В соответствии **с ГОСТ Р 27005-2010** «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», особое внимание следует уделять источникам угроз, происходящих от деятельности человека.

Задание на самостоятельную подготовку: изучить ГОСТ Р 27005-2010 в полном объеме и быть готовым им руководствоваться в ходе учебного процесса.

Третья группа угроз – угрозы по компонентам АИС, на которые нацелена угроза.

данные, программное обеспечение, аппаратное обеспечение, поддерживающая инфраструктура; угрозы, связанные с техническими и программными средствами, используемыми при разработке и эксплуатации информационных систем.

Угрозы компонентов АИС целесообразно рассматривать по трем группам отказов:

- отказ пользователей работать с ИС;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Применительно к *отказам пользователей* рассматриваются следующие угрозы:

нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями, и техническими характеристиками);

невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);

невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками *внутренних отказов* являются:

нарушение (случайное или умышленное) от установленных правил эксплуатации;

выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);

- ошибки при (пере)конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к *поддерживающей инфраструктуре* рекомендуется рассматривать следующие угрозы:

нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;

разрушение или повреждение помещений;

невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Четвертая группа угроз – угрозы по природе возникновения: *естественные (объективные) и искусственные (субъективные); техногенные угрозы, возникающие вследствие форс-мажорных обстоятельств*.

Естественные угрозы – это угрозы, вызванные воздействиями на АИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы – угрозы, вызванные деятельностью человека:

непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.

преднамеренные (умышленные) угрозы, связанные с целенаправленными устремлениями злоумышленников.

Основные непреднамеренные искусственные угрозы АИС:

- ✓ неумышленные физические действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
- ✓ неумышленная порча носителей информации;
- ✓ запуск программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование носителей информации, удаление данных и т.п.);
- ✓ самостоятельная установка и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- ✓ заражение компьютера вирусами, нарушающих целостность и доступность конфиденциальной информации;
- ✓ проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
- ✓ ввод ошибочных данных.

Основные преднамеренные искусственные угрозы АИС:

- ✓ физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);
- ✓ отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
- ✓ внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
- ✓ вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
- ✓ хищение носителей конфиденциальной информации
- ✓ чтение остаточной информации из оперативной памяти, внешних запоминающих устройств;
- ✓ незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);
- ✓ вскрытие шифров криптозащиты информации;
- ✓ незаконное подключение к телекоммуникационным системам и линиям связи.

На этом изложение учебного вопроса завершено.

Литература

1. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

2. ГОСТ Р 50922 «Защита информации. Основные термины и определения».

3. ГОСТ Р 27005-2010 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

4. Методика оценки угроз безопасности информации (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.).

Заключение

Из представленного учебного материала необходимо уяснить термины в области «угрозы информации» и классификацию данной категории.

Доцент кафедры БИТ Д.Власкин