УДК 004.056

О МЕТОДИКЕ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ БДУ ФСТЭК

© 2022 А. П. Гаврющенко[1], А. В. Масленников[2]

[1]кандидат технических наук, доцент кафедры ПОВТАС
e-mail: lviyc@mail.ru
[2]доктор технических наук, профессор кафедры ПОВТАС
e-mail: mav@kliver.pro

Белгородский государственный технологический университет им. В. Г. Шухова

Рассмотрен порядок определения актуальных угроз информационной безопасности в соответствии с методическим документом «Методика оценки угроз безопасности информации» Федеральной службы по техническому и экспортному контролю (ФСТЭК) при практическом применении данной методики. Для более глубокого понимания процессов, этапы сопровождаются практическими примерами.

Ключевые слова: информационная безопасность, безопасность информации, банк данных угроз, актуальные угрозы.

ON THE METHODOLOGY FOR DETERMINING CURRENT THREATS TO INFORMATION SECURITY USING THE FSTEC DATABASE

© 2022 A. P. Gavrushchenko[1], A. V. Maslennikov[2]

[1]Candidate of Technical Sciences
[2]Doctor of Technical Sciences
e-mail: lviyc@mail.ru

Belgorod State Technological University named after V. G. Shukhov

The procedure for determining current threats to information security in accordance with the methodological document "Methodology for assessing threats to information security" of the Federal Service for Technical and Export Control (FSTEC) in the practical application of this methodology is considered. For a deeper understanding of the processes, the steps are accompanied by practical examples.

Keywords: information security, information security, threat database, current threats.

При развитии информационных технологий, которые незаменимо вошли во все сферы общества, также параллельно стали развиваться технологии информационной безопасности (ИБ).

В настоящее время нормативная база в области защиты информации Российской Федерации достаточно велика: это защита государственных информационных систем, защита критической информационной инфраструктуры, защита персональных данных и т.д. Все эти требования обязывают практически каждый объект, задействованный в данных сферах, соблюдать требования по защите своих информационных ресурсов.

Согласно уже давно сложившейся практике и в соответствии с принятыми законодательными и нормативными документами для обеспечения организационно-технических мер защиты информации ограниченного распространения специалистами по информационной безопасности производится выявление угроз безопасности информации (БИ), преобразуемой в сетях связи, информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах, информационных системах и автоматизированных системах управления (далее – объект информатизации).

Цель определения угроз достаточно проста – определение механизмов защиты информации объекта информатизации (ОИ), и для ее достижения необходимо проанализировать все доступные сведения об угрозах и уязвимостях. Для этого применяются источники, в которых содержатся сведения обо всех известных угрозах безопасности информации, уязвимостях и описания векторов (шаблонов) компьютерных атак. Данные сведения содержатся в базах данных, таких как Банк данных угроз безопасности информации, реестрах, перечнях и классификациях CAPEC, ATT&CK, OWASP, STIX, WASC и др. Все это представляет собой общедоступные знания, сформированные экспертами по информационной безопасности.

В ходе изучения содержимого указанных источников любой специалист по защите информации столкнется с массой сложностей, связанных с тем, как правильно применить весь объем накопленных знаний, изложенных в данных документах к конкретному объекту информатизации, и определить для него актуальные угрозы безопасности информации.

В данной статье предлагаются рекомендации по анализу угроз информационной безопасности, в соответствии со сравнительно недавно опубликованным документом от Федеральной службы по техническому и экспортному контролю – «Методикой оценки угроз безопасности информации» (утверждена ФСТЭК России 5 февраля 2021 г.) [1].

«Методика применяется для определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информационным системам персональных данных, значимым объектам критической информационной инфраструктуры Российской Федерации, информационным системам управления производством, используемым организациями оборонно-промышленного комплекса, автоматизированным системам управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [1].

Данная методика опирается на классический подход по оценке актуальных угроз, а именно: определение возможных рисков отрицательных последствий, которые возможны от реализации (возникновения) угроз информационной безопасности, выявление нарушителей как источника угроз, оценка возможностей нарушителя и формирование сценария реализации угроз. По сути все логично: определили риски, выявили нарушителя, определили его тактики и техники (сформировали сценарий) и, исходя из этих данных, решили, является угроза актуальной или нет.

Ниже рассмотрен подробнее данный процесс на практике, отмечены сложности, которые могут возникнуть при рассмотрении всех критериев по оценке угроз.

1. Обследование объекта информатизации

Фиксируется документально состав информационной системы (проводится инвентаризация средств вычислительной техники и сетей), который включает:

– описание сетей и систем (как объектов защиты) и их характеристики: назначение объекта информатизации; какие задачи (функции) он решает, состав обрабатываемой информации, является ли информация охраняемой в соответствии с законодательством, основные процессы (бизнес-процессы), для обеспечения которых создан ОИ;

– состав и архитектура ОИ: общесистемное программное обеспечение, прикладное программное обеспечение, программно-аппаратные средства, используемые средства защиты информации;

– подключение к сетям электросвязи: интернет, информационно-телекоммуникационным сетям иных организаций;

– технологии, используемые в ОИ: съемные носители информации, технология виртуализации, технология беспроводного доступа, мобильные технические средства, веб-серверы, технология удаленного доступа, электронная почта и др.

2. Определение вероятных отрицательных последствий от реализации (возникновения) угроз БИ

В ходе исследования и выявления актуальных угроз ИБ определяются деструктивные последствия, которые вероятны при реализации (возникновения) угроз БИ. Деструктивные последствия выявляются применительно к нарушению основных процессов, выполнение которых обеспечивает ОИ.

На основании определенных негативных последствий формируются риски (ущерб). Методика предлагает рассматривать типовые виды рисков (ущерб) в трех направлениях:

– ущерб, который может понести субъект;

– опасности, угрожающие юридическому лицу или индивидуальному предпринимателю, которые связанны с производственно-хозяйственной деятельностью;

– ущерб, который угрожает стране в области обеспечения обороноспособности государства, безопасности государства и внутреннему правопорядку, а также в других сферах деятельности.

Основная сложность в том, что методика не содержит инструментария, с использованием которого могут быть определены негативные последствия по тому или иному риску (ущербу), применимому к системе. Здесь оператор системы опирается исключительно на свои методологии: например, для 152-ФЗ оператор при обработке личных данных должен проводить оценку вреда, который может быть причинен субъектам персональных данных (п.5 ст.18.1). Также для объектов критической информационной инфраструктуры согласно Постановлению Правительства №127 от 2018 года определен перечень показателей критериев значимости, исходя из которого определяются последствия для системы.

Пример: информационная система автоматизирует процесс формирования расписания на прием к врачу для электронной регистратуры. В случае нарушения данного процесса негативными последствиями будут выступать невозможность (прерывание) предоставления медицинской помощи, а риск будет выражен ущербом физическому лицу, и возможно даже жизни и здоровью, так как может быть не вовремя диагностировано заболевание, и т.д.

3. Возможные объекты воздействия угроз безопасности информации

«В ходе оценки угроз безопасности информации определяются информационные ресурсы и компоненты объекта информатизации, несанкционированный доступ

к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации могут привести к негативным последствиям» [1].

На основании анализа полученных данных и данных по обследованию систем и сетей определяются направления применения информационных ресурсов и комплексированных систем и сетей, которые с большой долей вероятности могут являться объектами воздействия. Выявление объектов воздействия следует производить на аппаратном, системном и прикладном уровнях, на уровне сетевой модели взаимодействия, а также на уровне пользователей. В отношении каждого объекта воздействия определяются виды воздействия на него, которые могут привести к негативным последствиям.

Пример: объект воздействия – автоматизированные рабочие места пользователей; негативные последствия – нарушение конфиденциальности (утечка) персональных данных; виды воздействия – нарушение функционирования (работоспособности) программно-аппаратных средств автоматизированного рабочего места.

4. Источники угроз безопасности информации

Потенциальными источниками угроз могут выступать человеческий фактор, техногенные или стихийные носители угрозы безопасности.

Для ОИ важно определить вероятные антропогенные источники угроз безопасности информации, к которым могут относиться субъекты (группа лиц), реализующие угрозу информационной безопасности посредством несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты объекта информации.

Антропогенным источником угроз выступает нарушитель безопасности информации, которым может быть физическое лицо, случайно или преднамеренно совершившее действия, в результате которых возникает нарушение безопасности информации при ее обработке в информационных системах техническими средствами.

Различают внутреннего и внешнего нарушителей. Внутренним нарушителем считают нарушителя, который находится внутри информационной системы в начале процесса реализации угрозы. Внешним нарушителем считается нарушитель, который находится за пределами информационной системы в момент начала процесса реализации угрозы.

Для успешной реализации угроз в ИС внешний нарушитель должен определенным способом получить доступ к процессам, выполняемым в информационной системе. При этом все свои дальнейшие действия внешний нарушитель должен выполнять под именем образованного им нового или существовавшего ранее в системе субъекта.

К внутренним нарушителям, согласно ГОСТ 53113.1-2008, относят инсайдеров. При этом они могут следовать инструкциям субъектов, которые находятся за пределами информационной системы.

Для каждого вида нарушителей формируется цель реализации угроз безопасности информации и, исходя из данной цели, выдвигаются предположения об отнесении к числу возможных нарушителей.

Пример: объект информатизации – медицинская информационная система коммерческой лечебно-профилактической организации. Вид нарушителя – спецслужбы иностранных государств; возможные цели нарушителя – нанесение ущерба государству в области обороны, безопасности и правопорядка; предположения об отнесении к числу возможных нарушителей – цели не предполагают потенциальное наличие нарушителя, так как медицинская информационная система не может нанести какой-

либо ущерб государству в области обороны. Вид нарушителя – физические лица (злоумышленники); возможные цели нарушителя – получение выгоды (финансовой или материальной); предположения об отнесении к числу возможных нарушителей – возможные цели осуществления угроз безопасности информации предполагают наличие нарушителя, так как хакер может провести шифрование данных и вести финансовый шантаж.

Далее проводится сопоставление возможных нарушителей и их целей по реализации угроз БИ с вероятными негативными последствиями и видами рисков (ущерба) от реализации (возникновения) угроз БИ. По результатам сопоставления определяются актуальные нарушители по следующему принципу: «нарушитель признается актуальным, если возможные цели реализации нарушителем угроз безопасности информации могут привести к определенным для ОИ негативным последствиям и соответствующим рискам (видам ущерба)» [1].

Пример: вид нарушителя – физические лица (злоумышленники); цели нарушителя – получение выгоды (финансовой или материальной); вид риска (ущерба) – нанесение ущерба физическому лицу (финансовый, иной материальный ущерб физлицу, нарушение конфиденциальности (утечка), целостность личных данных). Из данного примера видно, что хакер при совершении угрозы безопасности информации может нанести ущерб физическому лицу или его личным данным, обрабатываемым на объекте информатизации.

Итогом проведенных мероприятий в рамках данного пункта является перечень актуальных нарушителей БИ и уровень их возможностей. Уровень возможностей конкретного нарушителя по реализации угроз БИ можно определить, используя таблицу 9.1 «Методики оценки угроз безопасности информации».

5. Способы реализации (возникновения) угроз безопасности информации

В процессе оценки угроз БИ должны определяться наиболее вероятные способы реализации угроз безопасности информации, посредством использования которых нарушителями, являющимися в данном случае актуальными, могут быть реализованы угрозы БИ на объекте информатизации.

Процесс определения наиболее вероятных способов реализации (возникновения) угроз БИ предполагает составление перечня рассматриваемых (возможных) способов реализации угроз безопасности. Основными способами реализации (возникновения) угроз безопасности информации могут быть: уязвимости программного обеспечения, вредоносное ПО, использование недекларированных возможностей ПО, закладки (программные и программно-аппаратные), атаки, ошибочные действия и др.

Необходимо определить интерфейсы объектов воздействия, которые определяются на основе изучения и анализа данных полученных в ходе обследования ОИ:

– об архитектуре, составе и условиях функционирования операционной системы;

– о группах пользователей ИС, их типов доступа и уровней полномочий.

Итогом процесса определения актуальных способов реализации (возникновения) угроз БИ является описание способов реализации (возникновения) угроз безопасности информации, которые могут использоваться актуальными нарушителями, и описание интерфейсов объектов воздействия, доступных для использования актуальным нарушителям.

Пример: вид нарушителя – отдельные физические лица (хакеры); категория нарушителя – внешний; объекты воздействия – сетевой трафик; доступные интерфейсы – каналы связи с внешними информационно-телекоммуникационными сетями; способы реализации – использование уязвимостей в конфигурациях сетей, ошибочные действия

в процессе создания и использования систем и сетей, в том числе при установке, настройке программно-аппаратных и программных средств, перехват трафика сети передачи данных, осуществление атаки типа «отказ в обслуживании».

6. Актуальные угрозы БИ

В ходе анализа и оценки угроз информационной безопасности определяются вероятные угрозы безопасности информации и производится их оценка на актуальность для объекта информатизации – актуальные угрозы безопасности информации.

В качестве исходного перечня угроз безопасности информации необходимо использовать банк данных угроз безопасности информации, сформированный ФСТЭК России (http://bdu.fstec.ru/) [2].

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.

Банк данных угроз безопасности информации не имеет иерархической структуры; если скачать сведения об угрозах в виде электронной таблицы, то там доступна сортировка по источникам угроз (нарушителю), объектам воздействия, последствиям. По сути, мы можем на первоначальном этапе отсеять угрозы, которые не применимы для нашего объекта информатизации.

Пример: В информационной системе не применяются платформы виртуализации и аппаратные средства виртуальной инфраструктуры, то есть отсутствуют объекты воздействия, такие как виртуальная машина или гипервизор, соответственно, угрозы, применимые для данных объектов, следует исключить из состава рассматриваемых.

Далее процесс выделения из оставшегося перечня угроз безопасности информации БДУ возможных угроз осуществляется по следующему принципу: угроза БИ признается возможной, если имеются нарушитель или иной источник угрозы, объект, на который осуществляется воздействие, способ реализации угрозы безопасности информации, и реализация угрозы может привести к негативным последствиям.

«Выглядит это следующим образом: $УБИ_i$ = [нарушитель (источник угрозы); объекты воздействия; способы реализации угрозы; негативные последствия]» [1].

Пример: $УБИ_i$ – Угроза аппаратного сброса пароля BIOS (УБИ.004); источник угрозы – внутренний нарушитель, обладающий базовыми возможностями, внутренний нарушитель, обладающий базовыми повышенными возможностями; объект воздействия – BIOS/UEFI; способы реализации угрозы – несанкционированный физический доступ и (или) воздействие на технические средства, машинные носители информации; негативные последствия – необходимость дополнительных (внеплановых) затрат на покупку товаров, выполнение работ или оказание услуг (в том числе закупка ПО, технических средств, вышедших из строя, работы по замене, настройке, ремонту указанных средств).

Из сформированного перечня возможных угроз для информационной системы необходимо провести оценку возможных угроз на предмет актуальности. Данные мероприятия проводятся по следующему принципу: угроза признается актуальной, если имеется хотя бы один сценарий реализации угрозы безопасности информации.

«Определение сценариев включает 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. Хотя в методике и представлен перечень основных

тактик и соответствующих им типовых техник, он может быть дополнен в ходе построения сценариев реализации угроз безопасности информации» [1].

Пример отнесения угрозы к актуальной: $УБИ_i$ – Угроза аппаратного сброса пароля BIOS (УБИ.004); источник угрозы – внутренний нарушитель, обладающий базовыми возможностями, внутренний нарушитель, обладающий базовыми повышенными возможностями; объект воздействия – BIOS/UEFI; способы реализации угрозы – несанкционированный физический доступ и (или) воздействие на технические средства, машинные носители информации; негативные последствия – необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Сценарии реализации угрозы – применяемая тактика 1: сбор информации о системах и сетях (тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации); техника: сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей; применяемая тактика 2: получение первоначального доступа к компонентам систем и сетей; техника: несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими).

Процесс определения угроз безопасности информации и отнесение их к актуальным достаточно трудоемкий, и для качественной оценки методика предполагает формирование экспертной группы, которая включает специалистов по информационной безопасности, специалистов по информационным технологиям и т.д. На наш взгляд, далеко не каждый оператор обладает квалифицированным персоналом, способным провести качественную оценку угроз, даже при наличии в штате единичного специалиста данные мероприятия могут приводить к занижению прогнозов и предположений при оценке угроз или наоборот к завышению, что может повлечь за собой непредвиденный ущерб (риски) или неоправданные расходы на нейтрализацию (блокирование) угроз, являющихся неактуальными.

Библиографический список

1. Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.). – 83 с.

2. Методический документ «Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России» (утв. Федеральной службой по техническому и экспортному контролю 26 июня 2018 г.). – 15 с.

3. *Зуев, С. В.* Основы информационной безопасности: учебное пособие / С. В. Зуев. – Симферополь: ФГАОУ ВО «Крымский федеральный университет им. В. И. Вернадского», 2020. – 100 с.