Оптимизация подходов

к выбору мер по защите промышленных объектов КИИ от угроз безопасности информации на основе БДУ ФСТЭК России

Владимир АКИМЕНКО,
руководитель Центра кибербезопасности критических инфраструктур, АО «ЭЛВИС-ПЛЮС»

Положения Федерального закона № 187-ФЗ от 26.07.2017 и принятых в соответствии с ним нормативных правовых актов устанавливают порядок определения требований и мер защиты объектов критической информационной инфраструктуры (КИИ) от угроз безопасности информации. Требования к составу и выбору мер защиты установлены приказом ФСТЭК России № 239 от 25.12.2017 (239-П).

Этот документ определяет порядок выбора мер по обеспечению безопасности значимых объектов КИИ, который включает:

а) определение базового набора мер по обеспечению безопасности значимого объекта (на основе установленной категории значимости объекта);

б) адаптацию базового набора мер по обеспечению безопасности значимого объекта;

в) дополнение адаптированного набора мер по обеспечению безопасности объекта дополнительными мерами (при необходимости).

Базовый набор мер по обеспечению безопасности значимого объекта КИИ подлежит адаптации в соответствии с угрозами безопасности информации (УБИ), признанными актуальными для рассматриваемого объекта КИИ. При адаптации базового набора мер каждой актуальной угрозе, включенной в модель угроз, сопоставляется мера или группа мер, обеспечивающих блокирование одной или нескольких УБИ или снижающих возможность ее реализации, исходя из условий функционирования значимого объекта КИИ. В случае если базовый набор мер не позволяет обеспечить блокирование (нейтрализацию) всех актуальных УБИ, в него дополнительно включаются меры защиты, приведенные в 239-П. Однако этот порядок формально не допускает возможности использования для обеспечения безопасности объекта КИИ набора мер защиты менее адаптированного базового набора. То есть дополнительные меры защиты применять можно, а уменьшать набор мер защиты менее базового набора – нельзя.

Структура состава обобщенных ОВ

Рис. 1.

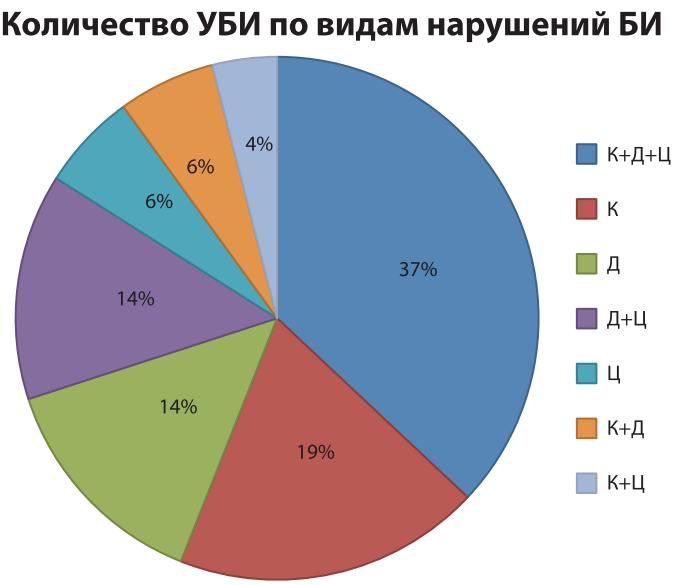

Рис. 2.

При моделировании УБИ для объектов КИИ ФСТЭК России предписывает (239-П, п. 11.1) в качестве исходных данных использовать банк данных угроз (БДУ), ведение которого осуществляется с 2015 года (bdu.fstec.ru).

Можно предположить, что базовый набор мер по обеспечению безопасности значимых объектов КИИ, включенный в 239-П, определялся на основе типовых моделей угроз безопасности информации, построенных с учетом лучших мировых практик, в том числе и с учетом угроз безопасности информации (БИ), включенных в БДУ ФСТЭК России.

В рамках настоящей статьи рассматривается сравнение набора мер защиты, определенных на основе анализа полного комплекса УБИ из БДУ ФСТЭК России, применимых для типовой структуры АСУТП, с минимально необходимым (базовым адаптированным) набором мер, определенным в соответствии с требованиями 239-П.

Как известно, УБИ рассматривается на основе цепочки: Источник угрозы (И) – Объект воздействия (ОВ) – Уязвимость (У) – Способ реализации угрозы (Р) – Последствия (П) (нарушение конфиденциальности (К), доступности (Д), целостности (Ц)).

В качестве источников УБИ в БДУ рассматриваются в основном антропогенные источники – нарушители. Нарушители характеризуются своей мотивацией и потенциалом. Анализ источников угроз показывает, что доля угроз, которые могут быть реализованы только нарушителем с высоким потенциалом, составляет всего 5%. Соответственно исключение подобных типов источников угроз несущественно влияет на состав рассматриваемых угроз.

Бессистемность в обозначении объектов воздействия в БДУ

Рис. 3.

Рис. 4.

(одни и те же, по сути, объекты называются в БДУ по-разному, например: оборудование указывается и как техническое средство, и как аппаратное обеспечение, и как сервер, АРМ, облачный сервер и т. п.) вызывает сложности при анализе угроз. Если обобщить приведенные понятия, то можно выделить группы объектов, указывающие на возможную цель воздействия нарушителя (рис. 1). Структура обобщенных объектов воздействия показывает, что основным объектом нарушения БИ выступает программное обеспечение (микропрограммное, системное, прикладное, сетевое, программное обеспечение гипервизора).

Как правило, в промышленных системах к технологической информации не предъявляются требования по обеспечению конфиденциальности, в связи с чем угрозы нарушения конфиденциальности могут быть признаны неактуальными, их доля может составлять до 20% от общего числа угроз (рис. 2), включенных в БДУ (за исключением угроз, направленных на получение доступа к аутентификационной информации).

Реализация УБИ возможна при наличии определенных факторов (уязвимостей), используя которые нарушитель может реализовать угрозы. Анализ сценариев реализации УБИ, указанных в БДУ, показывает, что основным способом реализации большого количества угроз является эксплуатация уязвимостей/«слабостей» программного обеспечения как общесистемного, так и микропрограммного, сетевого, прикладного и ПО гипервизора (рис. 3). Причем подобные «слабости»

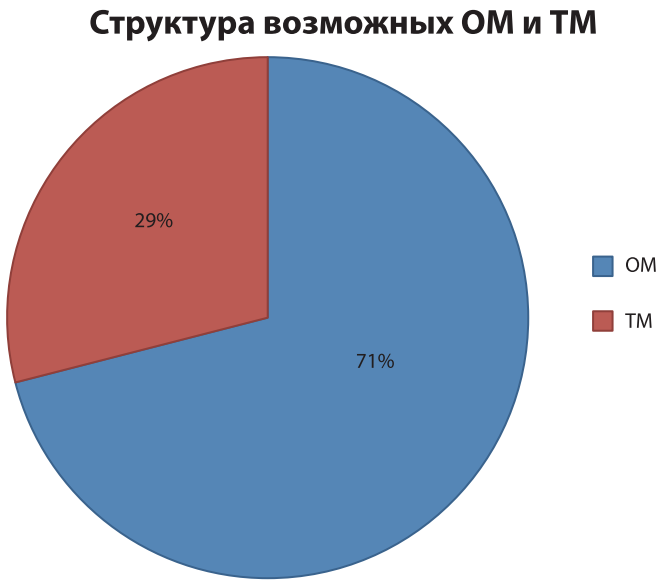

Рис. 5.

Доля возможных мер парирования УБИ по БДУ в общем количестве базовых мер, определенных 239-П

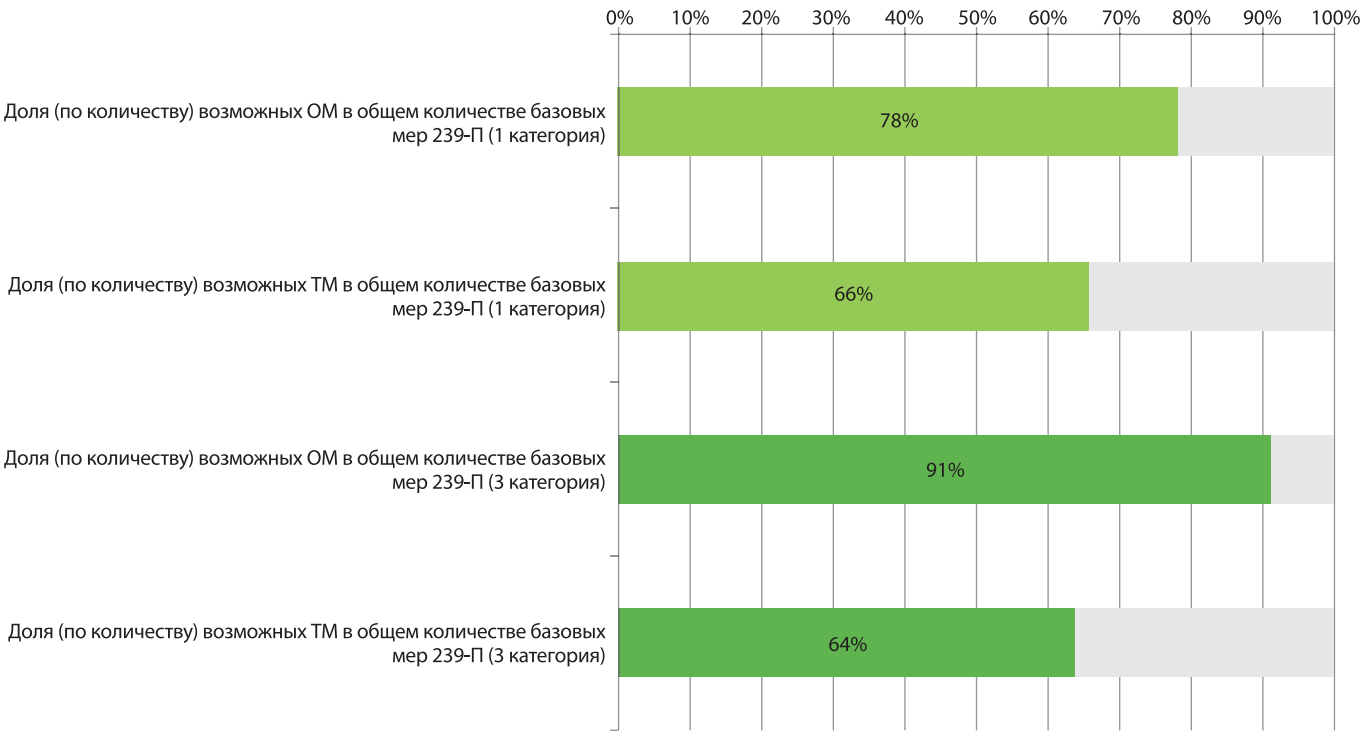

Рис. 6.

обусловлены не только нарушениями конфиденциальности или целостности обрабатываемых данных, но и нестабильной работой приложений, сбоями, некорректной обработкой данных, отсутствием защиты от ошибочных действий пользователей и другими функциональными уязвимостями.

Выбор мер парирования УБИ предполагает знание не только общей структуры средств автоматизации и порядка функционирования объекта КИИ, но и понимание модели обработки и хранения информации, потоков данных, технологий обработки и обмена данными между компонентами системы, а также знание механизмов защиты от возможных угроз нарушения безопасности информации. Указанные обстоятельства предъявляют достаточно высокие требования к квалификации работников, осуществляющих анализ и выработку возможных мер парирования актуальных угроз безопасности информации.

Рассмотрев возможные способы и механизмы нейтрализации указанных выше факторов и проведя их ранжирование, можно получить возможный перечень мер (рис. 4), обеспечивающих блокирование (снижение вероятности реализации) УБИ, указанных в БДУ.

При этом количество возможных технических мер защиты составляет примерно третью часть всех предполагаемых к внедрению мер (рис. 5). Они достаточно понятны, широко применяются в информационных системах как корпоративного, так и промышленного сегментов (средства межсетевого экранирования, антивирусная защита, средства управления доступом, регистрация событий, резервное копирование и восстановление).

Существенный вклад в нейтрализацию угроз вносят организационные меры, связанные с определением требований по защите, регламентацией процессов обеспечения и контроля безопасности объектов КИИ и установлением ответственности за обеспечение и нарушение правил безопасной работы с информационными ресурсами и средствами объекта КИИ.

Сопоставляя возможные меры парирования УБИ, входящие в БДУ, с базовым набором мер, определенным 239-П, а также учитывая предположения и ограничения, которые были указаны в настоящей статье, можно сделать вывод, что набор базовых мер, определенный 239-П, превышает состав мер, которые необходимы для парирования УБИ, включенных в состав БДУ (рис. 6).

Настоящий анализ может говорить о возможности оптимизации состава мер обеспечения безопасности объектов КИИ, установленного 239-П, путем проведения моделирования УБИ и выбора необходимых мер их нейтрализации.

При этом следует не забывать, что ответственность за соблюдение требований по обеспечению безопасности объектов КИИ несет субъект КИИ. ■