УДК 004.056.5

Комбинирование разнородных деструктивных воздействий на информационную систему и противодействие атакам (на примере инсайдерской деятельности и DDoS-атаки)

Буйневич М. В.[1] ✉, **Моисеенко Г. Ю.**[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
[2]Министерство обороны РФ
Москва, 194064, Российская Федерация

Постановка задачи. *К настоящему времени специалистами по информационной безопасности наработан достаточный широкий пул механизмов и средств противодействия кибератакам практически для всех классов деструктивных воздействий на информационные системы, поэтому для нарушения относительного паритета «атака* ***vs*** *защита» злоумышленники усиливают натиск на системы обеспечения безопасности информации, комбинируя разнородные деструктивные воздействия, затрудняя тем самым способность к противодействию. Несмотря на значительное количество публикаций, посвященных подобному информационному противоборству, каких-либо научных исследований, анализирующих это относительно новое явление в части выявления границ комбинирования, а также способности к противодействию возможным комбинациям в открытом доступе не наблюдается.* ***Цель работы*** *– исследование феномена комбинирования разнородных деструктивных воздействий на информационную систему и противодействия таким атакам.* ***Используемые методы.*** *Исследуется возможность комбинирования качественно разнородных атак на информационную систему организации. В интересах классификации и выделения таких атак применяется аппарат категориального деления с использованием следующих пар: Человек* ***vs*** *Автомат, Внутри* ***vs*** *Снаружи, Единичный* ***vs*** *Множественный.* ***Результат.*** *Применение категориального деления позволило выделить восемь классов атак с позиции механизма их реализации; дана интерпретация каждого из классов и приведен пример.* ***Новизна.*** *Впервые рассмотрена комбинация двух на первый взгляд не связанных деструктивных воздействий – инсайдерской деятельности и DDoS-атаки; приведена их обобщенная схема, этапы проведения, а также сложности противодействия им.*

Ключевые слова: *информационная безопасность, комбинирование атак, категориальное деление, инсайдерская деятельность, DDoS-атака*

Введение

Защита собственной информационной системы (ИС) является одной из первоочередных задач для любой организации [1, 2]. Сложность ее решения заключается как в технологичности проводимых атак, так и в их изощренности. Так, например, злоумышленник может не только провести технически подготовленную атаку по какому-либо каналу (сетевому, физическому, иному) [3], но и

Библиографическая ссылка на статью:
Буйневич М. В., Моисеенко Г. Ю. Комбинирование разнородных деструктивных воздействий на информационную систему и противодействие атакам (на примере инсайдерской деятельности и DDoS-атаки) // Информационные технологии и телекоммуникации. 2023. Т. 11. № 3. С. 27–36. DOI: 10.31854/2307-1303-2023-11-3-27-36

Reference for citation:
Buinevich M., Moiseenko G. Combining of Heterogeneous Destructive Impact on the Information System and Countering Attacks (on Example by Insider Activity and DDoS-Attack). *Telecom IT*. 2023. Vol. 11. Iss. 3. PP. 27–36. (in Russian) DOI: 10.31854/2307-1303-2023-11-3-27-36

скомбинировать ее из нескольких деструктивных воздействий [4], имеющих качественно разную природу. В результате система защиты информации (СЗИ) вынуждена как реагировать по различным каналам проведения атаки (например, состоять из межсетевых экранов и систем контроля и управления доступом), так и обеспечивать согласованное противодействие [5, 6]. Злоумышленник же, наоборот, может стремиться использовать на первый взгляд не связанные способы деструктивных воздействий, затрудняя тем самым их обнаружение или комплексирование защитных мероприятий в единый вектор. В результате возникает в некотором смысле дополнительное информационное противоборство между атакующими и защищающими организационно-техническими системами (ОТС), как совокупностями людей и технических средств. Первая такая ОТС в интересах достижения своей цели стремится использовать все многообразие деструктивных воздействий (прямых или косвенных) на ИС – внедряя и эксплуатируя уязвимости в программном обеспечении, стараясь физически проникнуть внутрь охраняемого периметра, внедряя собственных агентов или манипулируя имеющимися сотрудниками организации и т. п. Вторая же ОТС, наоборот, все это многообразие воздействий пытается детектировать, анализировать, коррелировать, свести в единый вектор и выбрать соответствующий согласованный набор мер противодействия.

Далее будет дано обоснование содержания такого противоборства путем рассмотрения комбинации атак, проводимых злоумышленником по качественно разным каналам (разнородных деструктивных воздействий); будет более детально рассмотрена одна из таких комбинаций на первый взгляд абсолютно не сочетаемых деструктивных воздействий, а именно – осуществление инсайдерской деятельности [7] с одновременной подготовкой и/или проведением DDoS-атаки [8]. Также будет рассмотрено противодействие подобного рода комбинированным атакам.

Категориальное деление

Для исследования возможности комбинирования деструктивных воздействий вначале необходимо выделить сами элементы этих комбинаций, т. е. произвести их классификацию. Сама по себе корректная классификация любых объектов, а не только атак на ИС, является достаточно сложной методологической задачей; и при этом требуется оценить их качественную разнородность, позволяющую злоумышленнику затруднить работу СЗИ. Одним из подходов для решения задачи является аппарат категориального деления, суть которого заключается в дихотомическом разделении (однократном или многократном) множества объектов согласно их отношению к элементам-антагонистам категориальной пары [9]. Так, например, все участники рассматриваемой предметной области могут быть поделены на две группы – стремящиеся 1) нарушить информационную безопасность и 2) обеспечить защищенность информации.

Считается, что несмотря на определенный пул общепринятых категориальных пар, в каждой конкретной области они вводятся или интерпретируются ис-

DOI: 10.31854/2307-1303-2023-11-3-27-36
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_3/27-36.pdf

следователями собственным образом [10]. Так, исходя из практических соображений (в частности, минимизации количества выделенных подмножеств), окончательный выбор пар осуществляется экспертно. Можно произвести классификацию атак по механизму их реализации, выделив следующие категориальные пары (отметим, что это возможное деление, но не единственное):

1) по источнику угроз: Человек ***vs*** Автомат – согласно тому, кто осуществляет инициацию, последовательность действий, контроль и корректировку атаки;

2) по локации точки инициации: Внутри ***vs*** Снаружи – основываясь на том, откуда начинается атака по отношению к защищаемому периметру (очевидно, что конечная точка атаки, которой является ИС, расположена внутри периметра);

3) по масштабу проведения: Единичный ***vs*** Множественный – исходя из количества действий, выполняемых в рамках единой атаки.

Названия элементов пар выбраны таким образом, чтобы их первые буквы были отличны – это позволит использовать в качестве имен классов хорошо понятные и различимые трехбуквенные идентификаторы. Применение категориального деления по трем введенным категориальным парам позволяет выделить $2 \times 2 \times 2 = 8$ классов атак по механизму их реализации.

В доказательство обоснованности приведенного деления дадим краткую интерпретацию каждого класса, а также приведем наглядный пример; каждый класс будем записывать как последовательность элементов каждой из трех категориальных пар:

1) Человек + Внутри + Единичный (*сокр*. ЧВЕ) – осуществление атаки *человеком*, находящимся *внутри* охраняемого периметра путем *единичных* деструктивных воздействий (например, разовое уничтожение данных в ИС в рамках инсайдерской деятельности) [11];

2) Человек + Внутри + Множественный (сокр. ЧВМ) – осуществление атаки *человеком*, находящимся *внутри* охраняемого периметра путем *множественных* деструктивных воздействий (например, в рамках инсайдерской деятельности длительный сбор данных из ИС для накопления их критического объема и последующей передачи конфиденциальной информации третьим лицам) [12];

3) Человек + Снаружи + Единичный (*сокр*. ЧСЕ) – осуществление атаки *человеком*, находящимся вне (*снаружи*) охраняемого периметра путем *единичных* деструктивных воздействий (например, попытка незаконного проникновения на территорию организации злоумышленником для физического доступа к ИС) [13];

4) Человек + Снаружи + Множественный (*сокр*. ЧСМ) – осуществление атаки *человеком*, находящимся вне (*снаружи*) охраняемого периметра путем *множественных* деструктивных воздействий (например, массового применения социальной инженерии, направленной на сотрудников организации для выявления интересующей информации об используемой СЗИ с дальнейшим ее обходом) [14];

5) Автомат + Внутри + Единичный (*сокр*. АВЕ) – осуществление атаки программно-аппаратным средством (*автоматом*), находящимся *внутри* охраняемого периметра путем *единичных* деструктивных воздействий (например, запуск вредоносного программного обеспечения непосредственно в сети или на устрой-

ствах организации, попавшего туда каким-либо средством доставки (например, таким, как троян или почтовый вирус [15]);

6) Автомат + Внутри + Множественный (*сокр*. АВМ) – осуществление атаки программно-аппаратным средством (*автоматом*), находящимся *внутри* охраняемого периметра путем *множественных* деструктивных воздействий (например, полный перебор паролей к ИС с «зараженного» ПК непосредственно внутри организации с последующими попытками несанкционированного доступа) [16];

7) Автомат + Снаружи + Единичный (*сокр*. АСЕ) – осуществление атаки программно-аппаратным средством (*автоматом*), находящимся вне (*снаружи*) охраняемого периметра путем *единичных* деструктивных воздействий (например, выполнение эксплойта, направленного на сетевой взлом внешнего Web-доступа к ИС) [17];

8) Автомат + Снаружи + Множественный (*сокр*. АСМ) – осуществление атаки программно-аппаратным средством (*автоматом*), находящимся вне (*снаружи*) охраняемого периметра путем *множественных* деструктивных воздействий (например, распределенная DoS-атака, также известная, как DDoS) [18].

Комбинирование атак

Важным в применении именно такой классификации является то, что каждый класс атак имеет признаки (элементы категориальных пар), по которым может быть оценена его качественная «отличность» от другого класса. Так, если каждый из классов отличается от другого хотя бы по одной из категориальных пар, несоответствие всех элементов пар будет означать максимальную разнородность классов. Очевидно, существует четыре пары классов с полностью различными элементами, а именно: ЧВЕ и АСМ, ЧВМ и АСЕ, ЧСЕ и АВМ, ЧСМ и АВЕ.

Рассмотрим более детально одну из пар классов, которые согласно примененному категориальному делению являются максимально разнородными – ЧВЕ и АСМ, в качестве примеров которых была приведена инсайдерская деятельность и DDoS-атака. Суть первой атаки заключается в том, что в организации с ИС существует сотрудник, который стал нарушителем (явно или несознательно, например, по причине манипуляции), поскольку в рамках своих должностных обязанностей и/или пользуясь нахождением в охраняемом периметре произвел ряд деструктивных действий по нарушению информационной безопасности ИС. Суть второй атаки противоположна первой и заключается в автоматическом проведении за пределами защищаемого периметра массированных деструктивных воздействий (отправка огромного количества сетевых пакетов, использование большого числа сетевых узлов, выполнение непрерывной последовательности ресурсозатратных операций) для достижения отказа в обслуживании самой ИС, обслуживающих сервисов или техники организации; для этого, как правило, применяются Botnet – группы компьютеров, одновременно отправляющих множество сетевых пакетов на сетевой адрес (или сеть) жертвы.

Схематичное интуитивно понятное отображение применения комбинации двух атак (ЧВЕ и АСМ) на одну ИС организации представлено на рисунке 1.

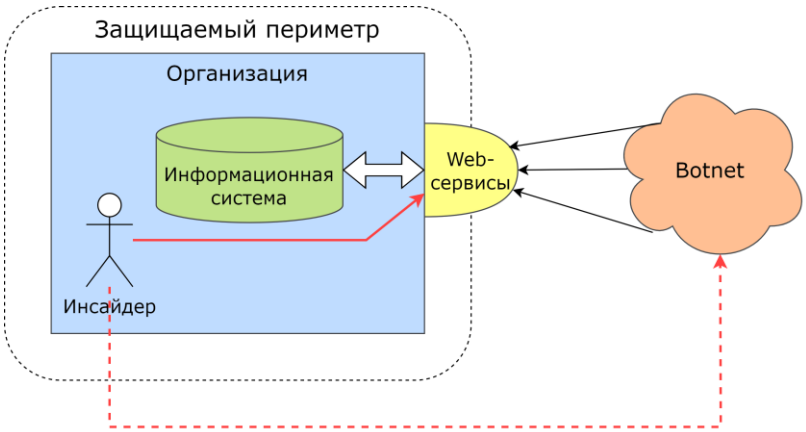

Рис. 1. Схематичное отображение применения комбинации двух деструктивных воздействий – инсайдерской деятельности и DDoS-атаки

Скомбинировать же эти два класса атак злоумышленник может следующим образом. Во-первых, находясь на рабочем месте и общаясь со службой сетевой безопасности, он может собрать информацию касательно обслуживания ИС, используемых механизмов ее защиты от DDoS-атак и их специфичных настроек [19]; например, что аппаратного обеспечения, на котором функционирует ИС, хватит для нормальной работы лишь при превышении количества запросов к ней не более, чем на 300 % от среднего показателя. Во-вторых, он гипотетически может уменьшить устойчивость ИС к DDoS-атакам; например, путем кратковременного (на время проведения атаки) физического вывода из строя кабеля питания резервного сервера (не говоря уже о самом сервере). И, в-третьих, снизив защищенность ИС, злоумышленник может извне провести непосредственную DDoS-атаку на ИС организации (как с собственных компьютеров, так и заказав данную услугу в даркнете). Соответственно, АСМ-атака будет проводиться и управляться человеком, находящимся внутри защищаемого периметра и выполняющим последовательность одиночных действий – ЧВЕ.

Выявление такой комбинированной (ЧВЕ + АСМ) атаки будет крайне сложным по следующим причинам. Во-первых, злоумышленник, как указывалась, действует сразу по двум каналам – физическому (или социальному) и сетевому, что требует от СЗИ поддержки по крайне мере анализа воздействий по этим каналам; например, внедрение в организации системы контроля и управления доступом более сложного типа, чем тривиальная рамка с металлодетектором и охрана без полноценного пропускного контроля (как на входе, так и в корпусах организации), а также установка межсетевого экрана с функционалом по детектированию (D)DoS-атак и системы резервирования. Во-вторых, определение факта совместного действия двух атак потребует интеграции соответствующих подсистем СЗИ в единый комплекс, способный скоррелировать различные сигналы от детекторов, например, сканирование внешних сетевых портов организации, недавний наем на работу неблагонадежного сотрудника, частое его нахождение в отделе сетевого администрирования, попытка подбора пароля внутри организации, резкое увеличение количества запросов к ИС, ошибки в работе си-

стемы резервирования, обнаружение вредоносного программного обеспечения [20] – все это может оказаться не отдельными «мелкими» инцидентами информационной безопасности, а частями хорошо спланированной комплексной атаки. И, в-третьих, противодействие таким атакам требует от СЗИ «аккуратного» (или даже точечного) воздействия, поскольку существенное ужесточение контрольно-пропускного режима повлияет как на потенциального инсайдера, так и на легальных пользователей, гипотетически снизив тем самым операционную эффективность всей организации; а необдуманное «вливание» денег в аппаратную часть ИС и связанных с ней Web-сервисовможет повлечь нецелесообразные (для коммерческой организации) финансовые траты.

Противодействие комбинированным атакам

Приведем один из возможных сценариев построения СЗИ, которая была бы способна противодействовать приведенному комбинированию атак (т. е. классов ЧВЕ и АСМ). Естественно, любая СЗИ с некоторой эффективностью скорее всего противодействует каждому из приведенных классов (как правило, в организации всегда присутствуют подсистемы контроля и управления доступом и сетевой безопасности), но в данном случае имеется в виду наличие синергетического эффекта – СЗИ должна быть способна отражать их комбинированное воздействие более эффективно (или, по крайне мере, результативнее), чем если бы атаки действовали не связанно.

Во-первых, очевидно, что в составе СЗИ должны быть подсистемы, ответственные за обнаружение деструктивных воздействий, связанных с каждой из комбинируемых злоумышленником атак. Например, необходимо иметь не только HR-подразделение, но и систему тестирования сотрудников (гипотетически как при устройстве на работу, так и периодически, как путем экспертного оценивания, так и на полиграфе и т. п.). Также потребуется подсистема сетевой безопасности с межсетевым экраном, настроенным на отражение DDoS-атак, возможностью экстренного подключения дополнительных мощностей. Подсистема же администрирования аппаратной части ИС в принципе должна уметь просчитывать и обеспечивать необходимые характеристики «железа» для обеспечения пользователей требуемым уровнем доступности к данным в ИС.

Во-вторых, для логического объединения двух разнородных деструктивных воздействий в единую комплексную атаку в СЗИ должна быть соответствующая подсистема (возможно, как организационно-техническая единица), которая помимо определения известных признаков таких деструктивных воздействий должна уметь предсказывать новые, пока еще потенциально не реализованные комбинации. Пример ее работы приводился выше и состоял в сопоставлении инцидентов из различных областей функционирования организации (работа персонала, администрирование оборудование, сетевой обмен и т. п.) и их сведение в единый гипотетический вектор атаки.

И, в-третьих, после определения проводимой комбинации атак необходимо произвести контратакующие воздействия, определяемые как действиями отдельных подсистем, так и согласованием их работы. Естественно, желательно

проведение превентивных мероприятий, в принципе не допускающих возможности таких атак. Например, помимо фильтрации пакетов, резервирования серверов и повышения лояльности сотрудников потребуется единая стратегия (или политика безопасности) по недопущению компрометации информации о системах защиты и программно-аппаратных характеристиках ключевых узлов ИС не только вне организации, но и среди сотрудников, которые могут потенциально стать инсайдерами.

Заключение

Исходя из вышеизложенного, можно предположить, что противодействие комбинированным атакам является крайне сложной задачей, требующей комплексного подхода при создании, внедрении, настройке и эксплуатации СЗИ. При этом, с позиции злоумышленника, проведение такого рода атак будет существенно проще, поскольку потребуется лишь осуществить корректное комбинирование деструктивных воздействий (фактически решить некую условную комбинаторную задачу), поскольку по отдельности атаки имеют большое количество реализаций, а злоумышленники (и в особенности, их организованные группы) – достаточно практического опыта. Все это продемонстрировано на примере двух разнородных деструктивных воздействий – инсайдерской деятельности и DDoS-атаки. Такая комбинация на первый взгляд не связанных деструктивных воздействий рассмотрена впервые.

Литература

1. Абдуллин Т. И., Баев В. Д., Буйневич М. В., Бурзунов Д. Д., Васильева И. Н. и др. Цифровые технологии и проблемы информационной безопасности: монография. СПб.: Санкт-Петербургский государственный экономический университет, 2021. 163 с.

2. Буйневич М. В., Васильева И. Н., Воробьев Т. М., Гниденко И. Г., Егорова И. В. и др. Защита информации в компьютерных системах: монография. СПб.: Санкт-Петербургский государственный экономический университет, 2017. 163 с.

3. Мостовой Р. А., Левина А. Б., Слепцова Д. М., Борисенко П. С. Атаки по сторонним каналам на мобильные телефоны // Вестник компьютерных и информационных технологий. 2019. № 12 (186). С. 46–53. DOI: 10.14489/vkit.2019.12.pp.046-053.

4. Дешина А. Е., Белоножкин В. И. Информационные риски в мультисерверных системах: атаки комплексного типа // Информация и безопасность. 2013. Т. 16. № 3. С. 335–344.

5. Буйневич М. В., Израилов К. Е., Покусов В. В., Ярошенко А. Ю. Основные принципы проектирования архитектуры современных систем защиты // Национальная безопасность и стратегическое планирование. 2020. № 3 (31). С. 51–58.

6. Израилов К. Е., Покусов В. В. Актуальные вопросы взаимодействия элементов комплексных систем защиты информации // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017): сборник научных статей VI Международной научно-технической и научно-методической конференции (Санкт-Петербург, 01–02 марта 2017 г.). СПб.: Санкт-Петербург-ский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2017. С. 255–260.

7. Власов Д. С. К вопросу о мотивации инсайдера организации и способах его классификации // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2022. № 1. С. 128–147.

8. Остапенко Г. А., Бурса М. В., Иванкин Е. Ф. Аналитическое моделирование процесса реализации DDoS-атаки типа HTTP-Flood // Информация и безопасность. 2013. Т. 16. № 1. С. 107–110.

9. Буйневич М. В., Израилов К. Е. Категориальный синтез и технологический анализ вариантов безопасного импортозамещения программного обеспечения телекоммуникационных устройств // Информационные технологии и телекоммуникации. 2016. Т. 4. № 3. С. 95–106.

10. Толстопятов А. А. Что такое кателогия // Вестник Ивановского государственного университета. Серия: Гуманитарные науки. 2013. № 3 (6). С. 101–108.

11. Поляничко М. А. Подход к оцениванию ценности информационных активов организации при противодействии инсайдерам // Электронные средства и системы управления: материалы докладов XV Международной научно-практической конференции. 2019. № 1-2. С. 126–128.

12. Кабанов А. С., Водолаженко А. А. Определение ценности и защита инсайдерской информации // Системы и средства информатики. 2020. Т. 30. № 2. С. 31–42.

13. Юркус А. Е. Повышение уровня информационной безопасности каталогов учетных записей при интеграции со СКУД в доменной структуре организации // REDS: Телекоммуникационные устройства и системы. 2018. Т. 8. № 4. С. 95–98.

14. Халилаева Э. И., Маслова М. А., Герасимов В. М. Система противодействия методам социальной инженерии в области информационной безопасности // Вестник УрФО. Безопасность в информационной сфере. 2023. № 2 (48). С. 54–61. DOI: 10.14529/secur230205

15. Исламгулова В. В., Радько Н. М., Шевченко И. В., Сурков И. А. Модели инфицирования элементов сетей посредством внедрения почтового червя // Информация и безопасность. 2016. Т. 19. № 2. С. 168–179.

16. Мигутина Е. А., Прокопович Ю. Ю., Кудрявцев О. А. Использование метода перебора паролей для взлома локальных документов // Наука молодых – будущее России: сборник научных статей 4-й Международной научной конференции перспективных разработок молодых ученых (Курск, 10–11 декабря 2019 г.). Курск: Юго-Западный государственный университет, 2019. С. 122–124.

17. Kasmi C., Lopes Esteves J. IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones // IEEE Transactions on Electromagnetic Compatibility. 2015. Vol. 57. Iss. 6. PP. 1752–1755. DOI: 10.1109/TEMC.2015.2463089

18. Krishna K. V., Reddy K. G. Classification of Distributed Denial of Service Attacks in VANET: a Survey // Wireless Personal Communications. 2023. Vol. 132. Iss. 2. PP. 933–964. DOI: 10.1007/s11277-023-10643-6

19. Уланов А. В., Котенко И. В. Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия // Защита информации. Инсайд. 2007. № 3 (15). С. 62–69.

20. Израилов К. Е., Гололобов Н. В., Краскин Г. А. Метод анализа вредоносного программного обеспечения на базе Fuzzy Hash // Информатизация и связь. 2019. № 2. С. 36–44. DOI: 10.34219/2078-8320-2019-10-2-36-44

Статья поступила 19 октября 2023 г.
Одобрена после рецензирования 20 декабря 2023 г.
Принята к публикации 25 декабря 2023 г.

Информация об авторах

Буйневич Михаил Викторович – доктор технических наук, профессор, ведущий научный сотрудник Управления организации научной работы и подготовки научных кадров Санкт-Петербургского государственного университета телекоммуникаций имени проф. М.А. Бонч-Бруевича.
E-mail: bmv1958@yandex.ru

Моисеенко Григорий Юрьевич – начальник направления Министерства обороны Российской Федерации. E-mail: mogreq@mail.ru

Combining of Heterogeneous Destructive Impact on the Information System and Countering Attacks (on Example by Insider Activity and DDoS-Attack)

Buinevich M.[1]✉, **Moiseenko G.**[2]

[1]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation
[2]Ministry of Defense of the Russian Federation
Moscow, 194064, Russian Federation

Problem statement. *By now, information security specialists have developed a sufficiently broad pool of mechanisms and means of countering cyberattacks for virtually all classes of destructive effects on information systems. Therefore, in order to break the relative parity "attack vs defense", attackers intensify their onslaught on information security systems by combining heterogeneous destructive influences, thus hampering the ability to counteract them. Despite a significant number of publications devoted to such information confrontation, there are no scientific studies devoted to analyzing this relatively new phenomenon in terms of identifying the limits of combinations, as well as the ability to counteract possible combinations in the public domain.* ***The aim of the work*** *is to study the phenomenon of combining heterogeneous destructive influences on the information system and counteracting such attacks.* ***Methods used.*** *The possibility of combining qualitatively heterogeneous attacks on the information system of the organization is studied. In order to classify and distinguish such attacks, categorical division apparatus is applied using the following pairs: Human vs Automaton, Inside vs Outside, Single vs Multiple.* ***Result.*** *The application of categorical division allowed to distinguish 8 classes of attacks from the position of their realization mechanism; the interpretation of each of the classes is given and an example is given.* ***Novelty.*** *The combination of two seemingly unrelated destructive influences – insider activity and DDoS-attack – is considered for the first time; their generalized scheme, stages of their implementation, as well as the complexity of counteraction to them are given.*

Keywords: *information security, combination of attacks, categorical division, insider activity, DDoS attack*

Information about Authors

Mikhail Buinevich − Dr. of Engineering Sciences, Leading Researcher at the Department of Scientific Work Organization and Scientific Personnel Training (The Bonch-Bruevich Saint-Petersburg State University of Telecommunications). E-mail: bmv1958@yandex.ru

Grigory Moiseenko − Head of Direction (Ministry of Defense of the Russian Federation). E-mail: mogreq@mail.ru

DOI: 10.31854/2307-1303-2023-11-3-27-36
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_3/27-36.pdf