ОБНАРУЖЕНИЕ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ НА СОТРУДНИКОВ ИНФРАСТРУКТУРНЫХ ОБЪЕКТОВ ПРИ РЕАЛИЗАЦИИ ЦЕЛЕВЫХ АТАК

Лапсарь А.П.[1], Кочемас Т.Г.[2]

Ключевые слова: *информационно-психологическое воздействие, целевая атака, методы обнаружения, инфраструктурный объект, поведенческий анализ, психотипы, психические свойства личности.*

Аннотация

Цель статьи: повышение безопасности инфраструктурных объектов на основе раннего обнаружения деструктивного информационно-психологического воздействия на их сотрудников.

Методы: компаративный анализ в рамках системного подхода; психоанализ личностных свойств; синергетика.

Полученный результат: проведен анализ особенностей целевых атак и методов их обнаружения. Сделан вывод о возможности использования методов социальной инженерии на подготовительной стадии реализации целевого воздействия на защищаемый объект. Рассмотрены психофизические свойства личности сотрудников объектов информационной инфраструктуры и способы воздействия на них со стороны злоумышленников. Предложен метод выявления информационно-психологического воздействия на сотрудников защищаемого объекта на начальной стадии целевого деструктивного воздействия, основанный на оценке изменения их психического состояния. Разработана схема реализации предложенного метода для интеграции в общую систему безопасности. Повышение безопасности объектов информационной инфраструктуры предлагается обеспечить за счет внедрения дополнительных организационных мер защиты.

Научная значимость: расширена область применения методов психоанализа на исследование безопасности информационных систем; синтезирован алгоритм раннего обнаружения целевых компьютерных атак на базе поведенческого анализа сотрудников инфраструктурного объекта.

DOI: 10.21681/1994-1404-2024-2-49-60

Введение

Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы[3] предполагает приоритетное развитие информационных технологий. Они охватывают все уровни общества, начиная от высших уровней государственного управления до повседневной деятельности отдельного гражданина.

Однако бурное развитие цифровизации, несмотря на очевидные преимущества, вызвало и отрицательные последствия, проявившиеся в существенном росте числа правонарушений в виртуальном пространстве. Это проявляется, среди прочего, смещением противоправных действий злоумышленников из области непосредственного физического контакта с объектом воздействия в виртуальную среду, позволяющую осуществлять деструктивные действия удаленно. В настоящее время деструктивные воздействия на информационную инфраструктуру представляют собой все более серьезную угрозу для функционирования ключевых элементов государственного управления и экономики. Все чаще используются методы гибридной войны, суть которых заключается в том, что противоборствующей стороне существенный урон наносится путем воздействия на информационные системы различного уровня и значимости.

[3] Утверждена Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

[1] ***Лапсарь Алексей Петрович****, кандидат технических наук, доцент, Ростовский государственный экономический университет, г. Ростов-на-Дону, Российская Федерация.*

E-mail: lapsarap1958@ mail.ru

[2] ***Кочемас Татьяна Георгиевна****, аспирант кафедры информационной безопасности, Ростовский государственный экономический университет, г. Ростов-на-Дону, Российская Федерация.*

E-mail: tkochemas@yandex.ru

В последние годы во всем мире прослеживается устойчивый тренд роста количества преступлений, совершенных в информационном пространстве, в частности, удаленных информационных воздействий на критическую инфраструктуру Российской Федерации. Стоит отметить, что значительная доля подобных воздействий — это целенаправленные атаки на объекты информационной инфраструктуры, реализующие управление производственными процессами в различных сферах [1—3]. Целевая или таргетированная атака представляет собой заранее спланированное управляемое продолжительное воздействие, имеющее конкретную цель, обладающее скрытностью и использующее различные, зачастую разрабатываемые под конкретную задачу, оригинальные инструменты и методы[4]. Все это делает ее одним из наиболее распространенных элементов современных киберпреступлений. Целевые атаки нацелены на получение информации ограниченного доступа, перехват управления жизненно важными элементами инфраструктуры, дестабилизацию внутриполитической обстановки и т. д., что предопределяет их широкое использование не только отдельными злоумышленниками и хакерскими группировками, но и спецслужбами враждебных государств [3—5].

Важность и актуальность проблемы защиты информационной инфраструктуры от киберпреступлений, а также сложность задачи повышения устойчивости инфраструктурных объектов к деструктивным информационным воздействиям приобрели первостепенное значение и обусловили их выход на государственный уровень. Вместе с тем проблема повышения устойчивости объектов инфраструктуры к компьютерным атакам и обеспечения их безопасности их функционирования рассматривается, как правило, только с технической точки зрения. Оценивается возможность оснащения объекта программными и техническими средствами, повышающими способность к противостоянию компьютерным атакам [3, 6—8]. Следствием этого явилось то, что предлагаемые модели объектов инфраструктуры не учитывают всех аспектов их функционирования, связанных с деятельностью их сотрудников. Государственное регулирование в области обеспечения безопасности объектов информационной инфраструктуры предусматривает применение сил и средств защиты от деструктивного воздействия, их состав назначается исходя из категории значимости. Однако при определении необходимых сил и средств защиты от деструктивного воздействия не учитываются особенности конкретного объекта, условия его функционирования, алгоритмы взаимодействия с обслуживающим персоналом и другие важные аспекты. В то же время имеющаяся статистика киберпреступлений говорит о том, что существенная их часть реализуется путем информационно-психологического воздействия на сотрудников инфраструктурных объектов. Отмечается, что в 2023 г. количество таких атак увеличилось на 20% по сравнению с 2022 г. Самыми распространёнными были атаки с использованием человеческого фактора. Таким образом, проблема защиты сотрудников от негативного влияния киберпреступников становится все более актуальной. Для успешного противодействия информационно-психологическому воздействию на сотрудников на начальной стадии целевой атаки требуется своевременное выявление воздействия на конкретного человека как неотъемлемого элемента инфраструктурного объекта и разработка методов повышения купирования такого воздействия.

Данная статья посвящена разработке метода раннего обнаружения деструктивного информационно-психологического воздействия на сотрудников защищаемых инфраструктурных объектов путем анализа изменения их психофизического состояния.

Особенности целевых атак на инфраструктурные объекты и методы их обнаружения

Сетевые воздействия на инфраструктурные объекты принято разделять на обычные или массовые, направленные одновременно на множество объектов, и целевые (таргетированные), предполагающие конкретный объект воздействия [9, 10]. Исследование целевых атак проведем с точки зрения их воздействия на информационные системы, играющие важную роль в обеспечении нормального функционирования различных значимых сфер[5] деятельности государства. Как отмечалось выше, целевые атаки — это атаки, нацеленные на конкретный выбранный инфраструктурный объект; важнейшей их особенностью является уникальность и сложность выявления на ранних стадиях.

Целевые атаки предполагают нацеленность на достижение нужного злоумышленнику результата и состоят из нескольких стадий. При организации целевых атак детально изучают особенности атакуемой информационной системы, выявляют слабые места, находят уязвимости, выясняют особенности системы защиты и построения самого объекта атаки для создания адаптивного вредоносного программного обеспечения, способного обойти защиту, проводят изучение персонала для воздействия на инфраструктурный объект через него. Такие атаки могут продолжаться длительный период времени, а их начало не всегда своевременно обнаруживается [11, 12]. Таким образом, главными отличительными признаками и особенностями целевых атак с точки зрения опасности являются следующие:

- такие атаки направлены на конкретный заранее выбранный объект;
- они реализуются длительный период времени;
- используемые приемы не использовались ранее на других объектах;

[4] Отчет Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q2/

[5] Указаны в Федеральном законе от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

– вредоносное программное обеспечение разрабатывается под конкретную атаку;
– широко применяются методы социальной инженерии[6].

Целевые атаки всегда следуют четко спланированному замыслу и выбранной стратегии, и, как правило, включают четыре основных стадии: подготовки, проникновения, закрепления и собственно реализации поставленных целей [11, 12]. Целевые атаки предполагают применение тех же приемов, что используются при проведении обычных. Основное отличие заключается в выявлении критических компонентов инфраструктурного объекта и последующего воздействия на них, а также в широком применении методов социальной инженерии для выявления характеристик объекта и особенностей его защиты. По результатам успешной целевой атаки использование полученных результатов может быть применено к другим аналогичным объектам[7]. В случае идентификации этой атаки средствами защиты атакованного объекта она остается опасной и для других, так как отсутствует достаточно сведений для ее обнаружения и детекции [2, 12, 13]. Реализованные методы и приемы, в том числе социальной инженерии, тиражируются при последующих целевых атаках.

Инфраструктурный объект можно условно разделить на две составляющие: программно-техническую и антропогенную. К первой относятся программные и аппаратные средства системы, в том числе и входящие в систему безопасности, а также их линии связи. Антропогенная составляющая включает сотрудников, имеющих различный уровень доступа к системе: администраторов, пользователей (операторов) и обслуживающий персонал. Таким образом, исходя из вышесказанного и по результатам анализа особенностей целевых атак, можно сделать вывод, что информационно-психологическое воздействие на сотрудников инфраструктурного объекта системы является их непременным элементом. Своевременное обнаружение и купирование таких воздействий и их последствий должно стать обязательной составляющей мероприятий по противодействию деструктивному воздействию (информационно-техническому и информационно-психологическому) и обеспечению безопасности инфраструктурных объектов всех уровней [14, 15].

В настоящее время проблема обнаружения целевых атак наиболее эффективно решается с использованием эвристических методов. Основным источником сведений для обнаружения целевых атак являются анализ процесса функционирования программно-технической составляющей информационной системы[8], а именно: сетевого трафика, потребляемых ресурсов, событий безопасности, целостности объектов файловой системы [4, 16]. Некоторая часть ресурсов инфраструктурного объекта выделяется для записи и анализа трафика, что позволяет собрать статистическую информацию и сформировать эталонную модель информационного обмена защищаемого объекта с открытыми сетями. Это дает возможность проводить мониторинг трафика и путем анализа определять динамику его изменения и тем самым выявлять признаки атак. Мониторинг и оперативный анализ сетевого трафика позволяют выявить обмен неопределенными пакетами, обнаружить в сети «незаконные» компьютеры или программы и т. д.[9] События безопасности находят отражение в журналах событий, где фиксируются все значимые события, в том числе сбои и ошибки в штатном функционировании объекта, попытки ошибочного ввода данных при входе в систему, а также все операции, совершаемые авторизованным пользователем под учетной записью.

Основными ресурсами, потребляемыми в процессе штатной работы инфраструктурного объекта, являются: процессорное время, объем памяти, задействование каналов ввода-вывода и периферийных устройств; мониторинг их изменения позволяет идентифицировать угрозу деструктивного воздействия в общем виде. Нарушение целостности объектов файловой системы предоставляет возможность определения изменений в программном обеспечении. Определение контрольных сумм и сравнение их с предыдущими результатами, хранящимися в базе данных, может сигнализировать о попытках модификаций. Тем самым выявляются попытки злоумышленников разместить вредоносные программы или создать бэкдор, что позволяет незаметно подключаться к системе и маскировать деструктивное воздействие.

Приоритетным способом обнаружения целевых атак является отслеживание аномалий в поведении инфраструктурного объекта, в запрашиваемых командах и реализуемых кодах. В рамках пессимистической оценки обнаруженные аномалии считаются проявлением компьютерной атаки, требующей незамедлительного применения алгоритмов защиты. Этот способ позволяет купировать атаки на ранних этапах их развития, однако он недостаточно эффективен при реализации подготовительной стадии целевой атаки. Анализ аномальной сетевой активности предполагает сравнение показателей процесса функционирования инфраструктурного объекта с эталонной моделью его поведения. Примером аномальной активности служит существенное повышение вычислительных затрат, неоднократное использование сторонних баз данных, блокировка пользовательского интерфейса или всего

[6] Передовая защита от сложных угроз и снижение риска целевых атак. URL: https://media.kaspersky.com/ru/businesssecurity/Kaspersky_Anti_Targeted_Attack_ Platform_Whitepaper_RU.pdf

[7] Безопасность объектов КИИ. URL: https://www.ptsecurity.com/ru/solutions/ bezopasnost-kii/

[8] Актуальные вопросы выявления сетевых атак. URL: http://www.infosecurity.ru/_gazeta/content/030211/article07.html

[9] Проблемы обработки статистики сетевого трафика для обнаружения вторжений в существующих информационных системах. URL: https://cyberleninka.ru/article/n/problemy-obrabotki-statistiki-setevogo-trafika-dlya-obnaruzheniya-vtorzheniy-v-suschestvuyuschih-informatsionnyh-sistemah

компьютера, нетипичные операции, неадекватная реакция на поступающую информацию и др.

Поведенческий анализ предусматривает сравнение текущей активности рабочих станций с эталонной моделью. Реакцией на выявление несоответствий является запрет на реализацию программного средства и блокирование входящего трафика, тем самым позволяя решать специфические задачи в области совершенствования систем безопасности инфраструктурных объектов. Следует отметить, что данный метод позволяет не только определять скомпрометированные аккаунты пользователей и проводить аудит прав доступа, но также обнаруживать и нейтрализовывать угрозы, связанные с инсайдерской деятельностью.

К наиболее популярным методам обнаружения целевых атак в настоящее время относят методы эвристического анализа, использующих не жестко заданные алгоритмы, а вероятностно-прогностические подходы[10]. Такие методы основываются на предположении о постоянном существовании угрозы деструктивного воздействия на инфраструктурный объект в произвольный момент времени. Априори делается предположение о том, что злоумышленники уже начали выполнение мероприятий начальной стадии целевой атаки.

Использование методами эвристического анализа нечетких и вероятностных алгоритмов обнаружения признаков целевых атак позволяет распространить их применение на антропогенную составляющую инфраструктурного объекта. Эвристический анализ на основе выявления подозрительных действий со стороны сотрудников позволяет получить вероятностную оценку осуществляемой целевой атаки. Обнаружение программно-аппаратными методами нестандартных и подозрительных операций в вычислительной составляющей инфраструктурного объекта, таких как изменение прав доступа, повышение привилегий учетных записей, открытие портов, добавление новых файлов или регистров, модификация реестров и т. д., может служить признаком непрофессиональных или преднамеренных действий сотрудников защищаемого объекта [4, 10, 16].

Основной недостаток эвристического анализа связан с «ложной тревогой» в ситуации, когда атака на объект защиты отсутствует. Однако при эксплуатации критически важных объектов считается, что издержки, связанные с профилактическими мероприятиями по обнаружению и устранению целевой атаки, существенно ниже, чем устранение последствий при ее успешной реализации.

Таким образом, решение задачи обнаружения и защиты от целевых атак на инфраструктурные объекты предполагает использование всех возможных методов или их сочетания.

Проведенный анализ показывает, что практически все имеющиеся методы раннего обнаружения и нейтрализации целевых атак на инфраструктурные объекты связаны с выявлением изменений в программно-аппаратной составляющей этой системы. Вместе с тем преднамеренные или неквалифицированные действия его сотрудников могут привести к обнулению системы безопасности атакуемого объекта и успешной реализации целевой атаки даже при отсутствии видимых уязвимостей. В условиях постоянно усиливающегося противоборства в информационном пространстве на значимых для государства и общества инфраструктурных объектах должны использоваться механизмы противодействия методам информационно-психологического воздействия на сотрудников. Однако решение этой задачи осложняется проблемой отсутствия надежных способов эффективного обнаружения деструктивного воздействия на сотрудников инфраструктурных объектов методами социальной инженерии.

Общая характеристика сотрудников инфраструктурного объекта

В антропогенной составляющей инфраструктурного объекта выделяют следующие категории сотрудников: администраторы, операторы, вспомогательный (обслуживающий) персонал.

Наибольшими правами доступа к информационным ресурсам, а, следовательно, и наибольшими возможностями воздействия на инфраструктурный объект обладают администраторы. При назначении на эти должности в организациях, эксплуатирующих критически важные объекты, кандидаты проходят тщательный отбор, проверяются на профессионализм, лояльность к организации, психическую устойчивость и т. д. Поэтому считается, что сотрудники категории «администраторы» слабо подвержены информационно-психологическому воздействию. Несмотря на повышенный интерес к этой категории со стороны злоумышленников, результаты информационно-психологического воздействия на них, как правило, незначительны, что позволяет исключить данную категорию из числа потенциальных объектов атаки.

Вспомогательный и обслуживающий персонал не имеет широкого доступа к ресурсам инфраструктурного объекта, а вмешательство в его работу неавторизованного пользователя легко обнаруживается, что не позволяет обеспечить скрытность целевой атаки.

В табл. 1 представлены характеристики администраторов, операторов и обслуживающего персонала как объекта потенциального интереса со стороны злоумышленников.

Как следует из табл. 1, наиболее критичными с точки зрения информационно-психологического воздействия считаются операторы. Эта самая многочисленная категория, с одной стороны, имеет достаточно широкие полномочия по взаимодействию с инфраструктурным объектом, а с другой — проверочные мероприятия при приеме на работу проводятся в усеченном объеме. Таким образом, категория операторов должна

[10] Эвристический анализ. URL: https://encyclopedia.kaspersky.ru/glossary/heuristic-analysis/

Таблица 1

Характеристика сотрудников инфраструктурного объекта

Сотрудники	Возможности	Требования при отборе	Мотивация к работе	Восприимчивость к ИПВ
Администратор	Высокие	Высокие	Высокая	Низкая (средняя)
Оператор	Средние	Средние	Средняя (низкая)	Средняя (высокая)
Персонал	Низкие	Низкие	Низкая (средняя)	Высокая (средняя)

априори рассматриваться в качестве потенциального объекта целевой атаки в форме информационно-психологического воздействия.

Рассмотрим основные характеристики операторов инфраструктурного объекта: психические свойства личности и ее психотипы. К основным психическим свойствам личности с точки зрения влияния на восприимчивость к деструктивному информационному воздействию относятся следующие [14, 15, 17]:

- Тревожность $T(t)$ — свойство, проявляющееся в возникающем по незначительным поводам чувстве волнения, нервозности, беспокойства.
- Ригидность $R(t)$ — свойство, характеризующее психологическую инерционность, негибкость.
- Фрустрированность $F(t)$ — состояние, возникающее, когда на пути к достижению цели встречаются непреодолимые препятствия, и проявляющееся в отчаянии, депрессии, отказе от активной деятельности и тому подобное.
- Агрессивность $A(t)$ — повышенная склонность к противодействию, отторжению любых правил, стремление энергично возражать по каждому поводу и тому подобное. Агрессивность и тревожность взаимосвязаны, поэтому в некоторых моделях изменения психического состояния сотрудников они учитываются как единая характеристика вида $A(t) = F_A\left[T(t)\right]$, где $F_A[...]$ — некоторый функционал.

Названные свойства оцениваются известными методами, например, путем тестирования по методике Айзенка [18] — выявление степени выраженности свойств, являющихся существенными компонентами личности: нейротизм, экстраверсия, интроверсия и психотизм. Анализ свойств личности сотрудников инфраструктурного объекта показывает, что с точки зрения информационной безопасности наиболее значимыми являются тревожность и агрессивность. Свойства ригидности и фрустрированности могут приводить к разнонаправленным последствиям в зависимости от конкретной обстановки и мотивации личности.

Очевидно, что деструктивное информационное воздействие будет направлено в первую очередь на изменение (усиление) первых двух свойств. С целью изменения в нужном направлении ригидности и фрустрированности злоумышленник может воздействовать не только непосредственно на сотрудника, но и на его окружение, в том числе и не связанное с его работой. Но в любом случае для повышения эффективности воздействия на сотрудников инфраструктурного объекта злоумышленник может использовать широкий набор методов и приемов.

Подверженность сотрудников инфраструктурного объекта информационно-психологическому воздействию как эффективность такого воздействия можно оценить по следующей формуле [20]:

$$P(t) = R(t)\frac{d^2G(t)}{dt} + Y(t)\frac{A(t)}{Z^2(t)} + \\ + R(t)\frac{2F(t)\left[R(t)A(t)\right]^{0,5}}{Z(t)F_D},$$

где $G(t)$ — уровень реакции оператора на психо-информационное воздействие, $Z(t)$ — временной параметр, характеризующий продолжительность и интенсивность воздействия, F_D — допустимый для данной категории сотрудников уровень фрустрации.

Традиционно выделяются четыре психотипа личности: флегматик, сангвиник, холерик и меланхолик [15, 17, 19]. Анализ психотипа сотрудников инфраструктурного объекта с точки зрения информационной безопасности представлен в табл. 2.

Приведенные в табл. 2 данные используются при назначении сотрудников на должности, связанные с обеспечением информационной безопасности. Проведя предварительную оценку психотипа, можно исключить сотрудников, относящихся к типу «холерик» и «меланхолик» из числа претендентов на должности администраторов.

Таким образов, проведя анализ общих психических характеристик персонала инфраструктурного объекта, можно констатировать, что наиболее вероятным объектом воздействия на начальной стадии целевых атак будет категория операторов, а основными психическими свойствами, влияющими на их подверженность информационно-психологическому воздействию, являются агрессивность и тревожность.

Таблица 2

Проявление свойств личности у каждого психотипа

Показатель	Флегматик	Сангвиник	Холерик	Меланхолик
Тревожность	нет	нет	да	да
Фрустрация	нет	да	нет	да
Агрессивность	нет	нет	да	нет
Ригидность	да	да	нет	нет

Способы реализации информационно-психологического воздействия на сотрудников инфраструктурных объектов

Считается, что при компьютерной атаке допускается некоторое ухудшение показателей функционирования инфраструктурного объекта без аварийного прекращения эксплуатации. Это позволяет выделить некоторое время для купирования целевой атаки и ликвидации ее последствий, причем это время напрямую зависит от интенсивности атаки и эффективности реагирования на нее созданной на объекте защиты системы безопасности. В свою очередь, реакция системы безопасности во многом обуславливается квалификацией сотрудников и адекватностью их реакции на возникающие угрозы. Мониторинг и оценка психофизического состояния сотрудников инфраструктурного объекта должны осуществляться непрерывно, а в условиях угрозы деструктивного информационного воздействия — усиливаться.

В целях выявления факта воздействия на операторов со стороны злоумышленников методами социальной инженерии и оценки его последствий проведем анализ способов такого воздействия на психофизические свойства сотрудников инфраструктурного объекта. Угрозы информационно-психологической безопасности реализуются через разработку, изготовление, распространение и применение деструктивных информационно-психологических материалов и специальных средств, а также совершенствование методов такого воздействия.

Основные психологические приемы, применяемые при атаках на сотрудников инфраструктурного объекта [15, 18]:

- отвлечение внимания — злоумышленник целенаправленно воздействует на оператора для переноса его внимания на другой объект;
- социальное соответствие — в общении с атакуемым сотрудником демонстрируется совпадение возраста, профессии, увлечений, положения в обществе и т. д.;
- обман — умышленное утаивание или искажение информации;
- срочность и ограниченность — изменение у атакуемого уровня осознания важности и правдоподобности полученной информации;
- потребности и желания — манипулирование данными личностными качествами в своих целях.

С использованием указанных приемов формируются конкретные атаки на антропогенную составляющую информационной системы. Наиболее распространенными видами атак считаются следующие[11] [19]:

- «ловля на живца» — злоумышленник оставляет приманку, например, инфицированный вирусом съемный накопитель информации;
- протекстинг — использование любого предлога для привлечения внимания жертвы с целью получения нужной информацию или провоцирования на совершение определенного действия;
- “quid pro quo” (услуга за услугу) — организация взаимодействия злоумышленника и атакуемого через средства коммуникации. Как правило, злоумышленник представляется техническим специалистом из службы поддержки;
- «троянский конь» — отправка атакуемому файлов, в программной составляющей которой находится вредоносный код. Одной из разновидностей троянского коня является инфицированная реклама;
- обратная социальная инженерия — создание неблагоприятной ситуации, при которой атакуемый сам обращается к злоумышленнику за помощью в ее разрешении;
- фишинг — отправка писем или сообщений от имени надежного источника. Данный вид атак наиболее распространен и имеет ряд разновидностей: поддельное сообщение, клон-фишинг (инфицирование настоящих сообщений), ложные лотереи, спир-фишинг или целевой фишинг, вэйлинг (маскировка под руководство организации).

При реализации воздействия на персонал инфраструктурного объекта злоумышленники используют множество конкретных приемов для сближения с атакуемым оператором[12] [18]:

- представление себя сотрудником (чаще всего неопытным), обращающимся с просьбой о помощи;

[11] Баришполец В.А. Области применения информационно-психологического воздействия // Информационные технологии. 2014. Т. 6. № 1. С. 52—79.

[12] Там же.

– представление себя представителем поставщика, партнерской компании, правоохранительных органов;
– представление себя кем-либо из руководства организации;
– представление себя разработчиком или производителем операционных систем или прикладных программ;
– предложение помощи со стороны сервисного центра;
– использование внутреннего сленга и терминологии;
– отправка инфицированных приложений к документу;
– использование фальшивого pop-up окна для провоцирования повторной аутентификации;
– предложение различных бонусов за регистрацию на сайте;
– записывание клавиш, которые оператор вводит на своем компьютере или в своей программе (кейлоггинг);
– подбрасывание различных носителей информации: или с вредоносным программным обеспечением, или документов в почтовый отдел организации;
– просьба принять, а затем переслать далее электронный документ;
– подстройка голосовой почты и т. д.

Результатами информационно-психологических воздействий могут стать следующие психологические последствия:
– негативное изменение психических свойств сотрудников;
– смещение базовых потребностей по «треугольнику Маслоу» [15];
– видоизменение каналов коммуникации между сотрудниками в сторону неофициальных;
– утратой доверия к имеющимся концепциям обеспечения защищенности объекта и формирование собственных.

Обобщая сказанное, можно сделать вывод, что в настоящее время имеется широкий и разнообразный набор приемов и методов негативного информационно-психологического воздействия на сотрудников инфраструктурного объекта с целью подготовки целевой атаки на него; последствия такого воздействия могут быть достаточно тяжелыми. Однако методы противодействия такому воздействию проработаны недостаточно, для успешного купирования угроз и защиты сотрудников инфраструктурного объекта требуется разработка методов раннего выявления начала информационно-психологического воздействия.

Метод выявления информационно-психологического воздействия на оператора в начальной стадии целевой атаки

Защиту инфраструктурного объекта от информационно-психологического воздействия рассмотрим с точки зрения решения двух задач: во-первых, это выявление персонала, изначально настроенного на сотрудничество со злоумышленниками (инсайдеров), а во-вторых — выявление сотрудников объекта, которые под влиянием деструктивного информационного воздействия изменяют свои психические свойства в направлении, нужном злоумышленнику.

Решение первой задачи предполагает анализ трех групп показателей: стационарных, периодически актуализируемых и динамических. Данные показатели позволяют определить, склонен ли работник к совершению нарушения, то есть определяется его предиспозиция[13].

К стационарным показателям относятся психологические и коммуникативные показатели, зависящие от личности человека. Методы оценки как психологических показателей (экстраверсия, способность прийти к согласию, сознательность, невротизм, открытость опыту), так и коммуникативных показателей (уровень общительности, склонность к соперничеству, сотрудничеству, компромиссу, склонность к приспособлению) хорошо известны.

К периодически актуализируемым относятся личностные показатели, поведенческие показатели, скрининговые показатели (данные полиграфа) и контекстные показатели. Данные показатели представляют собой многомерный набор количественных и качественных показателей, значения которых определяются на основе высказываний экспертов. Для обработки значений применяется нечеткое обобщение метода анализа иерархий[14].

Значения динамических показателей могут быть получены (системами DLP, IDS или SIEM) на основе данных вычислительной сети организации и ее информационных систем. Они отражают события, связанные с размножением документов, осуществлением доступа к ресурсам, скачиванием информации и другие.

Углубленная оценка предиспозиции проводится среди всех сотрудников инфраструктурного объекта при назначении на должность, что позволяет с большой долей вероятности определить сотрудников, потенциально склонных к инсайдерству, а также отобрать претендентов для назначения на должности администраторов.

Решение второй задачи осуществляется в течение всего времени функционирования инфраструктурного объекта. Выработка мер противодействия целевым атакам предполагает обнаружение изменения психических (психофизических) свойств операторов объекта защиты.

Как отмечалось выше, психическое состояние личности в *i*-ый момент времени можно охарактеризовать

[13] Бычков И.В., Веденеев В.С. Алгоритмы поиска инсайдеров в корпоративных компьютерных системах // Информация и безопасность. 2013. Т. 16. № 2. С. 179—184.

[14] Саати Т. Принятие решений. Метод анализа иерархий. М. : Радио и связь, 1993. 278 с.

четырьмя основными свойствами: тревожностью, ригидностью, фрустрированностью и агрессивностью: $S_i\left[T_i(t), R_i(t), F_i(t), A_i(t), t_i\right]$. Под влиянием информационно-психологического воздействия набор психических свойств оператора с течением времени изменяется, что приводит к изменению общего состояния личности: $S_i\left[T_i(t), R_i(t), F_i(t), A_i(t), t_i\right] \xrightarrow{F_S, G_S} S_j\left[T_j(t), R_j(t), F_j(t), A_j(t), t_j\right]$.

Обнаружение такого изменения может служить косвенным признаком целевой атаки на операторов инфраструктурного объекта и основой для выработки компенсационных мер. В качестве критерия распознавания изменения психического состояния операторов $\Delta S\left[T(t), R(t), F(t), A(t), t\right]$ можно использовать величину этого изменения. Тогда при условии превышения априори заданного значения $\Delta S\left[T(t), R(t), F(t), A(t), t\right] > \Delta S_{зад}\left[T(t), R(t), F(t), A(t), t\right]$ делается вывод о целенаправленном воздействии в интересах проводимой атаки.

Изменение психического состояния персонала информационной системы проводится через некоторые, не обязательно равные, промежутки времени путем сравнения разности значений $\left\|S_i\left[T_i(t), R_i(t), F_i(t), A_i(t), t_i\right]\right\|$ и $\left\|S_j\left[T_j(t), R_j(t), F_j(t), A_j(t), t_j\right]\right\|$, где $\left\|S_i[...]\right\|$ и $\left\|S_j[...]\right\|$ вычисляются как нормы соответствующих векторов в многомерном пространстве; мерность определяется количеством исследуемых психических свойств личности оператора информационной системы.

В простейшем случае изменение оценивается как минимум по изменению одного свойства на уровень выше допустимого $\Delta S\left[\Psi(t), t\right] > \Delta S_{доп}\left[\Psi(t), t\right]$, где $\Psi(t)$ принимает одно значение из совокупности $\left\{T(t), R(t), F(t), A(t)\right\}$. Таким образом, оценка изменения психических свойств личности оператора осуществляется либо по выполнению одного из условий $\Delta T_i(t) > \Delta T_{доп}(t)$, $\Delta R_i(t) > \Delta R_{доп}(t)$, $\Delta F_i(t) > \Delta F_{доп}(t)$ или $\Delta A_i(t) > \Delta T_{доп}(t)$, либо по суммарному изменению общего психического состояния $\Delta S_i\left[\Psi(t), t\right]$.

Оценка изменения тревожности, ригидности, фрустрированности и агрессивности производится с учетом значимости каждого свойства и его влияния на обеспечение безопасности инфраструктурного объекта. Исходя из этого, для каждого свойства назначается индивидуальное значение уровня его допустимого изменения $\Delta S_{доп}\left[\Psi(t), t\right]$, а при оценке общего психического состояния значимость каждого свойства учитывается путем введения соответствующих весовых коэффициентов, индивидуальных для каждого оператора.

Одинаковые группы пользователей могут быть охарактеризованы в каждый момент времени групповым психическим состоянием $\Phi(t) = \left\{S_{1,t_0}(t), ..., S_{k,t_0+m\tau}(t)\right\}$, где k — количество пользователей в группе, τ — период оценки психического состояния пользователей, $m = \overline{(1, M)}$ — количество проведенных проверок в течение всего времени наблюдения.

Алгоритм выявления изменения психического состояния операторов инфраструктурного объекта представлен на рис. 1.

Выявление информационно-психологического воздействия на оператора осуществляется следующим образом. В начале исследования оценивается начальное состояние $S_0\left[T_0(t), R_0(t), F_0(t), A_0(t), t_0\right]$ оператора. Априори считаем, что его начальное психическое состояние находится в области допустимых значений для успешного исполнения своих обязанностей. Каждая последующая оценка психического состояния оператора проводится через установленные руководством организации промежутки времени τ. Полученное по результатам очередной проверки состояние $S_i\left[T_i(t), R_i(t), F_i(t), A_i(t), t_i\right]$ сравнивается с исходным. Изменение психического состояния $\Delta S\left[T(t), R(t), F(t), A(t), t\right]$ сравнивается с априори установленным допустимым. При условии незначительных изменений в пределах допуска пользователь продолжает работу, через установленное время проводится очередная оценка. Полученное очередное значение психического состояния $S_{i+1}\left[T_{i+1}(t), R_{i+1}(t), F_{i+1}(t), A_{i+1}(t), t_{i+\tau}\right]$ сравнивается с предыдущим $S_i\left[T_i(t), R_i(t), F_i(t), A_i(t), t_i\right]$, после чего процедура повторяется. Это же значение $S_{i+1}[...]$ сравнивается также с исходным $S_0[...]$. Результат сравнения позволяет не только оценить текущее психологическое состояние оператора, но и отследить тренд на его изменение.

Признаками информационно-психологического воздействия на персонал информационной системы является одно из событий:

- изменение хотя бы одного из психических свойств персонала на уровень выше допустимого значения $\Delta T_i(t) > \Delta T_{доп}(t)$, $\Delta R_i(t) > \Delta R_{доп}(t)$, $\Delta F_i(t) > \Delta F_{доп}(t)$ или $\Delta A_i(t) > \Delta T_{доп}(t)$;
- изменение суммарного изменения общего психического состояния выше допуска $\Delta S_i\left[\Psi(t), t\right] > \Delta S_{доп}\left[\Psi(t), t\right]$;
- появление негативного тренда на изменение психического состояния выше некоторого уровня $\dfrac{\Delta S_i\left[\Psi(t), t\right]}{\Delta t} > \left(\dfrac{\Delta S_i\left[\Psi(t), t\right]}{\Delta t}\right)_{доп}$.

Для подтверждения признака проведения целевой атаки на инфраструктурный объект параллельно проводятся технические мероприятия по их обнаружению по аналогии с [16].

После обнаружения факта изменения психического состояния проводится ряд организационных мероприятий, направленных на недопущение развития ситуации в негативном русле и купирование результатов деструктивного информационно-психологического воздействия. К ним относится организация дополнительных занятий, проведение индивидуальных и груп-

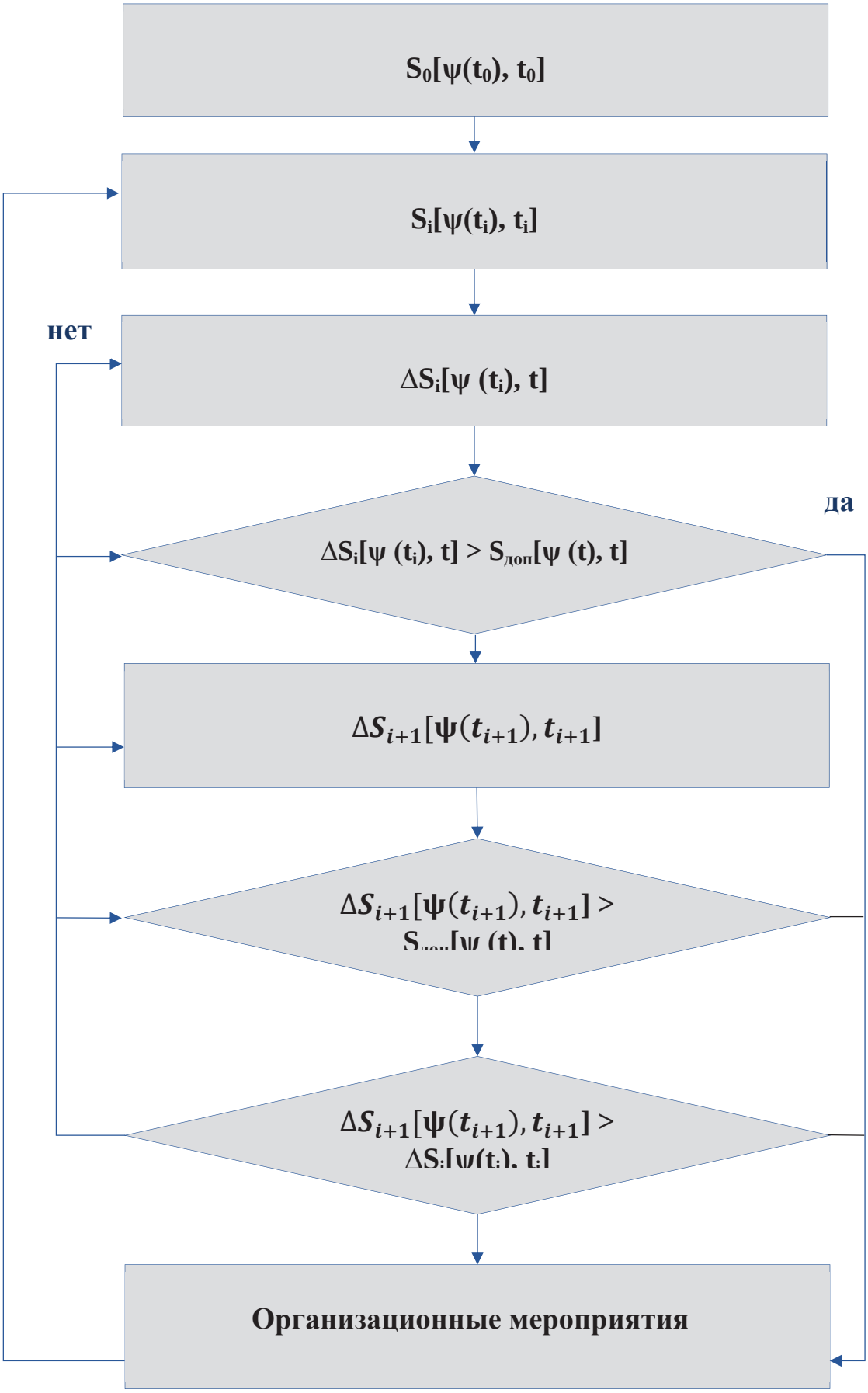

Рисунок 1. Алгоритм выявления изменения психического состояния

повых инструктажей, привлечение профессиональных психологов, сокращение времени между плановыми оценками состояния персонала, усиление контроля за работой операторов и другие аналогичные мероприятия, направленные на поддержания устойчивого психического состояния персонала. Обязательным условием должно быть более пристальное наблюдение за сотрудниками, наиболее подверженными информационно-психологическому воздействию. При необходимости могут привлекаться сотрудники службы безопасности объекта защиты и профессиональные психологи.

Заключение

Тенденция на увеличение объема, интенсивности и сложности деструктивных воздействий на инфраструктурные объекты, отмечаемая в последние годы, продолжит сохраняться и в дальнейшем. Методы и способы целевых атак на важные объекты защиты также продолжают совершенствоваться, с приоритетом развития приемов информационно-психологического воздействия. Несмотря на достаточно обширный аппарат оценки психологического состояния индивида, его применение в области обеспечения защиты объектов от деструктивного информационного воздействия не нашло широкого применения. В свете сказанного выше внедрение в практику информационной безопасности предложенного метода обнаружения целевых атак на стадии их подготовки может стать дополнительным инструментом противодействия злоумышленникам.

В данной работе проведен анализ особенностей целевых атак и методов их обнаружения. Сделан вывод об использовании методов социальной инженерии на подготовительной стадии реализации целевого воздействия на защищаемый объект. Рассмотрены психофизические свойства личности сотрудников объектов информационной инфраструктуры и способы воздействия на них со стороны злоумышленников. Предложен метод выявления информационно-психологического воздействия на сотрудников защищаемого объекта, основанный на оценке изменения их психического состояния. Разработана схема реализации предложенного метода для интеграции в общую систему безопасности. Повышение безопасности объектов информационной инфраструктуры предлагается повысить за счет внедрения дополнительных организационных мер защиты.

Метод реализуется преимущественно организационными мерами, не требует специальной подготовки в области медицины, психиатрии и психоанализа. Специалисты службы безопасности объекта защиты, назначенные для реализации предложенного метода, могут получить базовые навыки тестирования и обработки результатов тестов для оценки состояния операторов в ходе краткосрочного обучения.

Развитие предложенного метода выявления информационно-психологического воздействия на оператора в начальной стадии целевой атаки может идти в направлении автоматизации обработки результатов обследования операторов на предмет оценки их психического состояния, построения многофакторной модели устойчивости оператора к деструктивному воздействию, а также разработки и внедрения системы мониторинга психофизических показателей.

Литература

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Д.П. Зегжды. М. : Горячая линия — Телеком, 2022. 560 с.
2. Васильева В.И., Кириллова А.Д., Кухарев С.Н. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) // Вестник УрФО. Безопасность в информационной сфере. 2018. № 4. С. 66—74.
3. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. 2018. № 2. С. 2—15.
4. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. М. : Горячая линия — Телеком, 2023. 240 с.
5. Смирнов С.И., Киселёв А.Н., Азерский В.Д., Кумуржи Г.М. Комплексная методика проведения расследования инцидента информационной безопасности // Защита информации. Инсайд. 2023. № 2 (110). С. 14—26.
6. Израилов К.Е., Буйневич М.В. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 2. Алгоритм, модель и эксперимент // Вопросы кибербезопасности. 2023. № 4 (56). С. 80—93. DOI: 10.21681/2311-3456-2023-4-80-93 .
7. Котенко И.В., Дун Х. Обнаружение атак в интернете вещей на основе многозадачного обучения и гибридных методов сэмплирования // Вопросы кибербезопасности. 2024. № 2. С. 10—21.
8. Липатников В.А., Шевченко А.А., Мелехов К.В., Ткачев Д.Ф. Методика повышения защищенности сети передачи данных объектов критической информационной инфраструктуры при многоэтапных атаках // Информационно-управляющие системы. 2024. № 1. С. 44—55.

9. Шелухин О.И., Рыбаков С.Ю., Раковский Д.И. Классификация компьютерных атак с использованием мультифрактального спектра фрактальной размерности // Вопросы кибербезопасности. 2018. № 2. С. 2—15. DOI: 10.21681/2311-3456-2018-2-2-15 .
10. Коцыняк М.А. Математическая модель таргетированной компьютерной атаки / М.А. Коцыняк, О.С. Лаута, Д.А. Иванов // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 2. С. 73—81. DOI: 10.24411/2409-5419-2018-10261 .
11. Смирнов С.И. Метод обнаружения аномального поведения пользователя домена на основе интеллектуального анализа событий безопасности // Защита информации. Инсайд. 2022. № 3 (111). С. 56—83.
12. Корнеева Е.В., Федин Ф.О. Модель процесса обработки событий информационной безопасности на объекте критической информационной инфраструктуры // Вестник компьютерных и информационных технологий. 2023. № 7. С. 53—60.
13. Кондаков С.Е., Рудь И.С. Модель процесса проведения компьютерных атак с использованием специальных информационных воздействий // Вопросы кибербезопасности. 2021. № 5. С. 12—20. DOI: 10.21681/2311-3456-2021-5-12-20 .
14. Овчаренко М.С., Беспарточный А.Д. Психологические аспекты киберпреступности // Актуальные исследования. 2023. № 36 (166). С. 97—99.
15. Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. 4-е изд., перераб. и доп. М. : Горячая линия — Телеком, 2020. 636 с.
16. Лапсарь А.П., Назарян С.А., Владимирова А.И. Повышение устойчивости объектов критической информационной инфраструктуры к целевым компьютерным атакам на базе параметрического моделирования // Вопросы кибербезопасности. 2022. № 2. С. 39—51. DOI: 10.21681/2311-3456-2022-2-39-51 .
17. Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита. М. : Издательство МГУ, 1997. 344 с.
18. Пазухина А.П. Социальная инженерия, ее техники и меры противодействия // Молодой ученый. 2019. № 22 (260). С. 61—62.
19. Гончаров И.В., Паринов П.А. Модели информационно-психологического воздействия // Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2017. № 3. С. 65—71.

DETECTING INFORMATION AND PSYCHOLOGICAL INFLUENCE ON EMPLOYEES OF INFRASTRUCTURE FACILITIES WHEN TARGETED ATTACKS ARE PERFORMED

Aleksei Lapsar', *Ph.D. (Technology), Associate Professor, Rostov State University of Economics, Rostov-on-Don, Russian Federation.*
E-mail: *lapsarap1958@ mail.ru*

Tat'iana Kochemas, *Ph.D. student at the Information Security Department of the Rostov State University of Economics, Rostov-on-Don, Russian Federation.*
E-mail: *tkochemas@yandex.ru*

Keywords: *information and psychological influence, targeted attack, detection methods, infrastructure facility, behavioural analysis, psychological types, mental properties of personality.*

Abstract

Purpose of the paper: enhancing the security of infrastructure facilities based on early detection of destructive information and psychological influence on their employees.

Methods used in the study: comparative analysis within the system approach, psychological analysis of personality traits, the synergy method.

Study findings: features of targeted attacks and methods for detecting them were analysed. A conclusion was made that using social engineering methods was possible at the preparation stage of a targeted attack on a protected object.

Psychophysical properties of the personalities of employees of information infrastructure facilities and ways used by intruders to influence them were considered. A method is put forward for identifying information and psychological influence on the employees of a protected object at the initial stage of targeted destructive influence, it is based on an assessment of changes in their mental state. An implementation plan for the method was worked out, with a view of integrating it into the general security system. It is proposed to secure enhancing the security of information infrastructure facilities by dint of applying additional organisational measures of protection.

Research significance: the application of methods of psychological analysis is expanded to studying information systems security, and an algorithm is developed for early detection of targeted computer attacks based on the analysis of behaviour of employees of the infrastructure facility.

References

1. Kiberbezopasnost' tsifrovoi industrii. Teoriia i praktika funktsional'noi ustoichivosti k kiberatakam. Pod red. D.P. Zegzhdy. M. : Goriachaia liniia – Telekom, 2022. 560 s.
2. Vasil'eva V.I., Kirillova A.D., Kukharev S.N. Kiberbezopasnost' avtomatizirovannykh sistem upravleniia promyshlennykh ob"ektov (sovremennoe sostoianie, tendentsii). Vestnik UrFO. Bezopasnost' v informatsionnoi sfere, 2018, No. 4, pp. 66–74.
3. Zegzhda D.P., Vasil'ev Iu.S., Poltavtseva M.A., Kefeli I.F., Borovkov A.I. Kiberbezopasnost' progressivnykh proizvodstvennykh tekhnologii v epokhu tsifrovoi transformatsii. Voprosy kiberbezopasnosti, 2018, No. 2, pp. 2–15.
4. Erokhin S.D., Petukhov A.N., Piliugin P.L. Upravlenie bezopasnost'iu kriticheskikh informatsionnykh infrastruktur. M. : Goriachaia liniia – Telekom, 2023. 240 s.
5. Smirnov S.I., Kiselev A.N., Azerskii V.D., Kumurzhi G.M. Kompleksnaia metodika provedeniia rassledovaniia intsidenta informatsionnoi bezopasnosti. Zashchita informatsii. Insaid, 2023, No. 2 (110), pp. 14–26.
6. Izrailov K.E., Buinevich M.V. Metod obnaruzheniia atak razlichnogo geneza na slozhnye ob"ekty na osnove informatsii sostoianiia. Chast' 2. Algoritm, model' i eksperiment. Voprosy kiberbezopasnosti, 2023, No. 4 (56), pp. 80–93. DOI: 10.21681/2311-3456-2023-4-80-93 .
7. Kotenko I.V., Dun Kh. Obnaruzhenie atak v internete veshchei na osnove mnogozadachnogo obucheniia i gibridnykh metodov semplirovaniia. Voprosy kiberbezopasnosti, 2024, No. 2, pp. 10–21.
8. Lipatnikov V.A., Shevchenko A.A., Melekhov K.V., Tkachev D.F. Metodika povysheniia zashchishchennosti seti peredachi dannykh ob"ektov kriticheskoi informatsionnoi infrastruktury pri mnogoetapnykh atakakh. Informatsionno-upravliaiushchie sistemy, 2024, No. 1, pp. 44–55.
9. Shelukhin O.I., Rybakov S.Iu., Rakovskii D.I. Klassifikatsiia komp'iuternykh atak s ispol'zovaniem mul'tifraktal'nogo spektra fraktal'noi razmernosti. Voprosy kiberbezopasnosti, 2018, No. 2, pp. 2–15. DOI: 10.21681/2311-3456-2018-2-2-15 .
10. Kotsyniak M.A. Matematicheskaia model' targetirovannoi komp'iuternoi ataki. M.A. Kotsyniak, O.S. Lauta, D.A. Ivanov. Naukoemkie tekhnologii v kosmicheskikh issledovaniiakh Zemli, 2019, t. 11, No. 2, pp. 73–81. DOI: 10.24411/2409-5419-2018-10261 .
11. Smirnov S.I. Metod obnaruzheniia anomal'nogo povedeniia pol'zovatelia domena na osnove intellektual'nogo analiza sobytii bezopasnosti. Zashchita informatsii. Insaid, 2022, No. 3 (111), pp. 56–83.
12. Korneeva E.V., Fedin F.O. Model' protsessa obrabotki sobytii informatsionnoi bezopasnosti na ob"ekte kriticheskoi informatsionnoi infrastruktury. Vestnik komp'iuternykh i informatsionnykh tekhnologii, 2023, No. 7, pp. 53–60.
13. Kondakov S.E., Rud' I.S. Model' protsessa provedeniia komp'iuternykh atak s ispol'zovaniem spetsial'nykh informatsionnykh vozdeistvii. Voprosy kiberbezopasnosti, 2021, No. 5, pp. 12–20. DOI: 10.21681/2311-3456-2021-5-12-20 .
14. Ovcharenko M.S., Bespartochnyi A.D. Psikhologicheskie aspekty kiberprestupnosti. Aktual'nye issledovaniia, 2023, No. 36 (166), pp. 97–99.
15. Manoilo A.V., Petrenko A.I., Frolov D.B. Gosudarstvennaia informatsionnaia politika v usloviiakh informatsionno-psikhologicheskoi voiny. 4-e izd., pererab. i dop. M. : Goriachaia liniia – Telekom, 2020. 636 s.
16. Lapsar'A.P., Nazarian S.A., Vladimirova A.I. Povyshenie ustoichivosti ob"ektov kriticheskoi informatsionnoi infrastruktury k tselevym komp'iuternym atakam na baze parametricheskogo modelirovaniia. Voprosy kiberbezopasnosti, 2022, No. 2, pp. 39–51. DOI: 10.21681/2311-3456-2022-2-39-51 .
17. Dotsenko E.L. Psikhologiia manipuliatsii: fenomeny, mekhanizmy i zashchita. M. : Izdatel'stvo MGU, 1997. 344 s.
18. Pazukhina A.P. Sotsial'naia inzheneriia, ee tekhniki i mery protivodeistviia. Molodoi uchenyi, 2019, No. 22 (260), pp. 61–62.
19. Goncharov I.V., Parinov P.A. Modeli informatsionno-psikhologicheskogo vozdeistviia. Vestnik VGU. Seriia: Sistemnyi analiz i informatsionnye tekhnologii, 2017, No. 3, pp. 65–71.