УДК 004.056 Вестник УрФО № 1(47) / 2023, с. 81–97

Голушко А.П., Жуков В.Г.

DOI: 10.14529/secur230108

ПРЕЦЕДЕНТНОЕ ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ КОНФИГУРИРОВАНИЯ, ОБЕСПЕЧИВАЮЩИХ РЕАЛИЗАЦИЮ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

В статье рассматривается решение задачи определения параметров конфигурирования объектов информатизации и применяемых средств защиты, которые бы могли обеспечить противодействие компьютерным атакам. В качестве источника информации о сценариях проведения атак предлагается использовать результаты прецедентного анализа из базы знаний MITRE ATT&CK. Продемонстрирована возможность интеграции результатов прецедентного анализа информации о тактиках и техниках проведения атак организованными группами злоумышленников в процесс определения и настройки параметров конфигурирования и оценки эффективности реализуемых мер защиты с учетом существующих требований безопасности. Представлены результаты применения предлагаемого подхода на примере отдельно взятой тактики.

Ключевые слова: *защита информации, проектирование системы защиты информации, меры защиты информации, MITRE ATT&CK, эмуляция активности злоумышленника, Atomic Red Team.*

PRECEDENT DEFINITION OF CONFIGURATION PARAMETERS THAT ENSURE THE IMPLEMENTATION OF INFORMATION SECURITY MEASURES

The article is devoted to the scientific and practical problem of determining the configuration parameters of information infrastructure and its information security system, which could provide counteraction to modern methods of computer attacks. It is proposed to use MITRE ATT&CK matrices as a source of systemized analysis of computer attacks. The article presents the analysis results of systematized source applicability, advantages and limitations, an approach to integration into determining the of configuration parameters and evaluating the effectiveness of security system.

Keywords: *MITRE ATT&CK, FSTEC, information security system development, determination of security system configuration parameters, emulation of malicious activity, Atomic Red Team.*

1. Введение

При проектировании системы защиты информации перед специалистами ставится задача определения параметров настройки программного обеспечения, включая программное обеспечение средств защиты, обеспечивающих выполнение требований безопасности и нейтрализацию актуальных угроз. Наряду с требования нормативно-методических документов применяются существующие рекомендации – лучшие практики конфигурирования.

Однако набор параметров конфигурирования должен не только соответствовать требованиям нормативных документов и лучшим практикам, но также обеспечивать противодействие современным методам компьютерных атак. При внедрении системы защиты и проведении оценки соответствия эффективность системы защиты должна подтверждаться.

Основная сложность для владельцев информационных систем, лицензиатов ФСТЭК России и ФСБ России, осуществляющих проектирование и внедрение систем защиты, заключается в необходимости определять конфигурации, опираясь не только на знания о структурно-функциональных характеристиках системы, применяемых информационных технологиях и потенциально возможных угрозах безопасности, но опираясь также и на реальные прецеденты атак, наиболее объективно определяющие ландшафт угроз, условия их реализации и эффективные меры противодействия действиям злоумышленников.

Актуальность решаемой задачи обусловлена необходимостью единства подхода к обеспечению информационной безопасности – внедрению знаний о методах совершения атак, об активности преступных групп и используемых злоумышленниками инструментах – на всех этапах создания системы защиты: от оценки актуальных угроз и формирования требований до проектирования и внедрения системы защиты.

В результате, на этапе проектирования системы защиты должно определяться кон-

кретное содержание реализуемых мер защиты для предотвращения реализации современных компьютерных атак, а также должны обеспечиваться методы и средства оценки эффективности принятых мер.

2. Описание текущего подхода к процессу конфигурирования программного обеспечения и средств защиты информации

2.1 Описание текущего подхода

В рамках данной работы рассматривается подход к созданию системы защиты информации (далее – СЗИ), осуществляемый в соответствии с требованиями законодательства РФ [1–7].

В процесс создания СЗИ входят в т.ч. следующие мероприятия:

– определение угроз безопасности информации (далее – УБИ), реализация которых может привести к нарушению безопасности информации, и разработку на их основе модели угроз (этап – формирование требований к защите информации);

– определение требований к СЗИ (этап – формирование требований к защите информации);

– проектирование СЗИ (этап – разработка системы защиты информации).

Параметры конфигурирования определяются при проектировании СЗИ и фиксируются в проектной и/или эксплуатационной документации.

При определении требований к параметрам конфигурирования программного обеспечения (далее – ПО) и средств защиты информации (далее – СрЗИ) основными источниками, как правило, являются:

– эксплуатационная документация на ПО, программно-технические средства и СрЗИ;

– рекомендации разработчиков и исследовательских центров (CIS Benchmarks [10]);

– формуляры СрЗИ;

– нормативно-методические документы, например, «Меры защиты информации в государственных информационных системах» [8];

– структурно-функциональные характеристики информационной системы (далее – ИС);

– сведения об уязвимостях и способах реализации УБИ в соответствии с Банком данных угроз безопасности ФСТЭК России (далее – БДУ ФСТЭК России) [11] и региональными или отраслевыми нормативно-правовыми актами;

– международные базы данных об уязвимостях в ПО, например, CVE [12] и др.

На этапе проектирования СЗИ перед специалистами ставится задача определить такие состав и содержание мер защиты (в том числе параметры конфигурации), которое позволит выполнить минимально предъявляемые требования и обеспечить нейтрализацию актуальных УБИ.

На практике специалистам приходится применять «экспертный подход» для определения параметров конфигурации, которые бы могли обеспечить нейтрализацию актуальных УБИ. Такой подход заключается в необходимости поиска информации во внешних источниках и руководстве собственным профессиональным опытом. Меры защиты в большей степени реализуются путем определения параметров в соответствии с лучшими практиками, например, [10] и требованиями регулятора, например, [8]. При этом отсутствует единый методологический подход к проведению контроля на предмет, позволяют ли эти параметры в действительности блокировать современные УБИ.

Дополнительно необходимо отметить, что в связи с применением СрЗИ уровня узла сети, частично или полностью заменяющих стандартные средства операционных систем, при проектировании СЗИ преимущественно осуществляется выбор конфигураций СрЗИ, в то время как штатные средства операционных систем могут оставаться с настройками «по умолчанию» или с теми параметрами, которые применяются для задач системного администрирования.

2.2 Пример определения параметров конфигурации

Для того, чтобы наглядно продемонстрировать возможные результаты интеграции систематизированных сведений о мерах противодействия современным техникам компьютерных атак (далее – КА) в процесс определения параметров конфигурирования, предлагается рассмотреть пример определения параметров конфигурации для некоторой произвольной ИС.

Для рассмотрения были выбраны меры защиты из нескольких групп в соответствии с документом [4], для каждой из которых приведены сведения о выбранных параметрах конфигурирования и потенциально нейтрализуемых УБИ (табл. 1).

При определении параметров конфигурирования специалистами используются ис-

Таблица 1

Выбор параметров конфигурации системы защиты

№ п/п	Меры защиты информации[1]	Параметры конфигурирования	Внутренние документы, отражающие состав и содержание мер защиты в ИС	Нейтрализуемые УБИ[2]
1	ИАФ.1 Идентификация и аутентификация пользователей, ИАФ.3 Управление идентификаторами, ИАФ.4 Управление средствами аутентификации	– Максимальный период неактивности до блокировки экрана: 15 минут; – Количество неудачных попыток аутентификации: от 3 до 10 попыток; – Минимальная длина: не менее 6-8 символов; – Требования к сложности пароля: наличие строчных, прописных букв, цифр и символов – Срок действия пароля: не более 180/120/90/60 дней	Описание технологического процесса обработки информации Положение по идентификации и аутентификации	УБИ.008 Угроза восстановления аутентификационной информации УБИ.100 Угроза обхода некорректно настроенных механизмов аутентификации
2	УПД.2 Реализация необходимых методов, типов и правил разграничения доступа, УПД.4 Разделение полномочий пользователей, администраторов, УПД.5 Назначение минимально необходимых прав и привилегий	– Контроль отсутствия административных прав у учетных записей пользователей на уровне системного и прикладного ПО – Назначение необходимых прав на файлы и каталоги – Назначение необходимых прав в прикладном ПО для обеспечения выполнения трудовых обязанностей	Матрица разграничения прав доступа Инструкции администратора ИБ, системного администратора, пользователей	УБИ.006 Угроза внедрения кода или данных УБИ.028 Угроза использования альтернативных путей доступа к ресурсам
3	ОПС.1 Определение запускаемых компонентов ПО, настройка параметров запуска, ОПС.2 Управление установкой компонентов ПО, определение компонентов, подлежащих установке	Настройка защищенной программной среды: – Прикладное ПО и его компоненты, которым разрешен запуск (например, Microsoft Office и средства чтения pdf документов в пользовательском сегменте, СУБД Postgree SQL, веб-сервер Nginx, docker-контейнеры в серверном сегменте) – Запрет запуска исполняемых файлов . exe и скриптов (.bat, PowerShell)	Перечень ПО и его компонентов, разрешенных к установке в ИС	УБИ.178 Угроза несанкционированного использования системных и сетевых утилит УБИ.188 Угроза подмены программного обеспечения

[1] Состав мер защиты информации формируется на этапе формирования требований к системе защиты информации и фиксируется в Техническом задании на создание системы защиты информации.

[2] В соответствии с требованиями законодательства РФ в качестве основного источника сведений об УБИ применяется БДУ ФСТЭК России, дополнительно могут применяться иные источники.

точники, которые предоставляют отдельно сведения о нейтрализуемых УБИ и уязвимостях [11, 12], требованиях к мерам защиты [8] и рекомендациях по настройке параметров ПО [10].

3. Выбор систематизированного источника информации о методах современных компьютерных атак для интеграции

На текущий момент становится важным интегрировать знания о проведенных КА по всему миру в процесс создания СЗИ, поскольку эти сведения формируют реальный ландшафт актуальных УБИ и могут служить источником эффективных мер противодействия действиям злоумышленников.

Это направление развития высоко оценивается и методически поддерживается регулятором. Такой практико-ориентированный подход теперь должен применяться на этапе разработки модели угроз в соответствии с новой методикой оценки угроз безопасности, утвержденной ФСТЭК России [9].

Согласно данной методики оценка актуальности угроз осуществляется посредством построения возможных сценариев их реализации. Сценарии реализации УБИ формируются из состава тактик и техник действий злоумышленников, которые были определены в результате апостериорного анализа инцидентов информационной безопасности. Проектируемая СЗИ должна обеспечить блокирование техник из состава актуальных сценариев реализации УБИ.

Совместными усилиями различных организаций в течение нескольких лет собирались и систематизировались знания о мерах противодействия актуальным УБИ, которые могут быть интегрированы в существующий процесс проектирования СЗИ в целях повышения их эффективности против современных КА.

Так, например, центр компьютерной безопасности Австралии (Australian Cyber Security Centre) выпускает рекомендации по конфигурированию операционных систем, веб-ресурсов и иных компонентов ИС [13], в т.ч. определяет меры, внедрение которых направлено на минимизацию рисков возникновения инцидентов в разных организациях [14].

В качестве основного источника для выбора безопасных конфигураций ПО серверов, рабочих станций и сетевого оборудования часто выступают рекомендации CIS Benchmarks [10].

Однако наиболее подходящим с точки зрения единства методологического подхода источником информации о мерах противодействия современным КА является систематизированная база знаний о тактиках и техниках действий злоумышленников Adversarial Tactics, Techniques & Common Knowledge (далее – ATT&CK), разработанная компанией MITRE [15].

ATT&CK представляет собой постоянно растущий систематизированный ресурс информации о результатах апостериорного анализа поведения злоумышленников при совершении КА. Общая структура MITRE ATT&CK представлена на рис. 1.

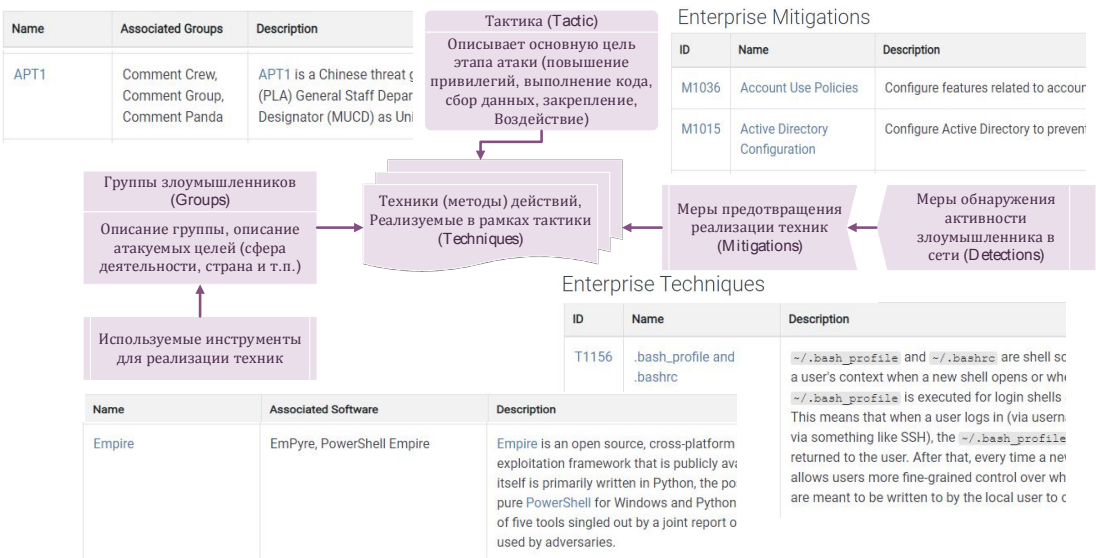

Рис. 1. Структура базы знаний MITRE ATT&CK

В рамках настоящей работы наибольший интерес представляют сведения о возможных мерах защиты и предотвращения возможности реализации техник (Mitigations).

В состав мер противодействия техникам, описанных в категории ATT&CK Enterprise, входит более сорока мер. Каждая мера имеет ссылки на нейтрализуемые с ее применением техники и соответственно суб-техники.

4. Анализ применимости ATT&CK к задаче определения конфигурации системы защиты информации

Представленные в ATT&CK Enterprise меры противодействия техникам могут быть соотнесены с мерами защиты, определяемыми в соответствии с требованиями документов [4–8]. Пример частичного сравнения мер защиты из [4] и [15] представлен в табл. 2.

Таблица 2

Соотнесение мер противодействия техникам КА и мер защиты, определяемых нормативно-методическими документами

№ п/п	Меры защиты ФСТЭК России	ATT&CK Mitigations
1	ИАФ.1 Идентификация и аутентификация пользователей, ИАФ.3 Управление идентификаторами ИАФ.4 Управление средствами аутентификации	M1032 Multi-factor Authentication M1027 Password Policies M1043 Credential Access Protection M1028 Operating System Configuration
2	УПД.1 Управление учетными записями, УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой), типов (чтение, запись, выполнение) и правил разграничения доступа УПД.4 Разделение полномочий УПД.5 Назначение минимально необходимых прав и привилегий УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	M1026 Privileged Account Management M1022 Restrict File and Directory Permissions M1024 Restrict Registry Permissions M1052 User Account Control M1018 User Account Management M1015 Active Directory Configuration M1028 Operating System Configuration M1054 Software Configuration
3	УПД.3 Управление информационными потоками между устройствами, сегментами ИС, а также иными ИС	M1037 Filter Network Traffic
4	ОПС.1 Определение запускаемых компонентов ПО, настройка параметров запуска, ОПС.2 Управление установкой компонентов ПО, определение компонентов, подлежащих установке ОПС.3 Установка только разрешенного к использованию ПО и его компонентов	M1038 Execution Prevention M1033 Limit Software Installation
5	АН3.1 Выявление, анализ уязвимостей и оперативное устранение АН3.2 Контроль установки обновлений ПО, АН3.3 Контроль работоспособности, параметров настройки и правильности функционирования ПО и СрЗИ	M1051 Update Software M1054 Software Configuration M1016 Vulnerability Scanning M1050 Exploit Protection M1015 Active Directory Configuration M1028 Operating System Configuration M1054 Software Configuration
6	СОВ.1 Обнаружение вторжений	M1031 Network Intrusion Prevention
7	ЗИС.17 Разбиение ИС на сегменты	M1030 Network Segmentation
8	ОДТ.4 Периодическое резервное копирование информации ОДТ.5 Обеспечение возможности восстановления информации с резервных носителей	M1053 Data Backup
9	УПД.17 Обеспечение доверенной загрузки средств вычислительной техники	M1046 Boot Integrity
10	ОЦЛ.1 Контроль целостности ПО, включая ПО СрЗИ	M1025 Privileged Process Integrity M1045 Code Signing

Чтобы подтвердить, что сведения, представленные в базе ATT&CK допустимо считать достаточно информативными для их интеграции в процесс определения параметров настройки ПО и СрЗИ необходимо провести дополнительный анализ уровня детализации состава и содержания мер противодействия техникам ATT&CK.

Для того, чтобы оценить рекомендации о мерах противодействия, в качестве примера рассмотрим несколько техник из состава тактики Lateral Movement. Сведения приведены в табл. 3.

Таблица 3 дополнена столбцом, содержащим сведения о мерах защиты согласно документу [4]. Требования к реализации обозна-

Таблица 3

Анализ уровня детализации представленных сведений о мерах противодействия техникам действий злоумышленников

№ п/п	Техника действий злоумышленника (ATT&CK)	Содержание угрозы	Меры противодействия по MITRE ATT&CK	Меры детектирования действий в сети	Меры защиты по приказам ФСТЭК России
1	T1077-Windows Admin Shares	Скрытые сетевые папки предоставляют возможность удаленного копирования файлов. Примеры: C$, ADMIN$, IPC$ Получение учетных данных администратора позволяет через SMB/RPC создавать назначенные задания, запуск служб и использовать WMI	(M1027) Внедрение парольной политики: создание сложных и уникальных паролей, использование разных паролей на учетных записях локального администратора, (M1026) запрет удаленного входа в систему встроенной учетной записи локального администратора (M1038) Ограничение с применением Software Restriction Policies возможности запуска ПО, которое может быть использовано для эксплуатации SMB и Admin Shares	Централизованный сбор и хранение журналов использования учетных данных для входа в системы Отслеживание действий удаленных пользователей, которые подключаются к Admin Shares, отслеживание инструментов и команд, которые используются для подключения к общим сетевым ресурсам, или осуществляют поиск удаленных систем	ИАФ.1, Идентификация и аутентификация пользователей, ИАФ.3 Управление идентификаторами ИАФ.4 Управление средствами аутентификации ОПС.1 Определение запускаемых компонентов ПО, настройка параметров запуска, ОПС.2 Управление установкой компонентов ПО, определение компонентов, подлежащих установке
2	T1028-Windows Remote Management	Реализуется путем возможности удаленного взаимодействия с машиной через службу WinRM с применением PowerShell или иных программ	(M1042) отключить службу WinRM (M1030) внедрение физической и/или логической сегментации сети. Внедрение DMZ для размещения интернет-сервисов (M1026) в случае если служба WinRM необходима, дефолтные настройки скорректировать - произвести настройку учетных записей, рабочих станций и серверов для разграничения прав доступа	Мониторинг использования WinRM – процессов и действий, выполняемых службой WinRM Соотнесение событий WinRM с другими связанными событиями.	УПД.1 Управление учетными записями пользователей, УПД.2 Реализация необходимых методов, типов и правил разграничения доступа ЗИС.17 Разбиение ИС на сегменты и обеспечение защиты периметров сегментов ИС

ченных мер приведены в документе [8] и включают в себя в т.ч. требования:

– ИАФ.1 (О) При доступе в ИС должна осуществляться идентификация и аутентификация пользователей и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей;

– ИАФ.1 (У.3) должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального/удаленного доступа в систему с правами привилегированных учетных записей (администраторов);

– ИАФ.3 (О) формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;

– ИАФ.3 (У.2) оператором должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования не более 90/45 дней;

– ИАФ.3 (У.3) оператором должно быть обеспечено использование различной аутентификационной информации (различных средств аутентификации) пользователя для входа в ИС и доступа к прикладному (специальному) ПО;

– ИАФ.4 (О) изменение аутентификационной информации, заданных их производителями и (или) используемых при внедрении СЗИ;

– ИАФ.4 (О) установление характеристик пароля: а) задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов; б) задание минимального количества измененных символов при создании новых паролей; в) задание максимального времени действия пароля; г) задание минимального времени действия пароля;

– УПД.1 (О) предоставление пользователям прав доступа к объектам доступа ИС, основываясь на задачах, решаемых пользователями;

– УПД.2 (У.1) в ИС правила разграничения доступа должны обеспечивать управление доступом субъектов при входе; (У.2) управление доступом субъектов к техническим средствам, устройствам, внешним устройствам; (У.3, У.4) управление доступом субъектов к объектам, создаваемым общесистемным, прикладным и специальным ПО.

В составе перечисленных требований, например, содержатся требования к паролям и однозначной идентификации пользователей, в т.ч. привилегированных, что коррелирует с мерами противодействия M1026 и M1027 из состава ATT&CK. Однако дополнительные рекомендации по предотвращению реализации атак на конкретные используемые технологии (в примере из таблицы – Windows Admin Shares, WinRM service) дополняют имеющиеся требования и могут быть внедрены при проектировании СЗИ.

Таким образом могут быть сделаны выводы, что сведения, представленные в матрице Enterprise MITRE ATT&CK, дополняют содержание мер защиты практическими рекомендациями, позволяющими определить необходимые параметры конфигурирования.

По результатам проведенного анализа, предлагается подход к интеграции знаний о мерах противодействия техникам КА в процесс определения параметров настройки ПО, включая ПО СрЗИ.

5. Описание предлагаемого подхода к интеграции знаний о мерах противодействия техникам компьютерных атак в процесс определения параметров конфигурирования системы защиты информации

Предлагаемый подход основывается на основных этапах создания (проектирования) СЗИ, которые осуществляются в соответствии с [1–7].

Интеграцию знаний о тактиках и техниках действий злоумышленников предлагается осуществлять после того, как определены минимальные требования к составу мер защиты в соответствии с [4–8].

Область действия подхода охватывает процесс определения параметров конфигурирования системного и прикладного ПО ИС и ПО СрЗИ.

Предлагаемый подход включает в себя следующие этапы:

1. Из общего состава мер защиты осуществляется выбор одной меры или группы мер, для которой необходимо определить минимальные требования по настройке и дополнительные рекомендации по противодействию техникам КА.

2. Определяются параметры настройки в соответствии с требованиями нормативно-методических документов (если требованиями предусмотрены конкретные значения параметров).

3. Осуществляется выбор категории мер противодействия (Mitigations) из состава MITRE ATT&CK, сопоставимой или соответ-

ствующей мерам защиты, выбранным на этапе 1.

4. Для выбранных на этапе 3 категорий мер противодействия к рассмотрению принимаются представленные в MITRE ATT&CK более детализированные рекомендации.

5. Далее во внешних источниках осуществляется поиск конкретных практических рекомендаций для реализации рекомендуемой меры противодействия (в случае если ATT&CK не содержит достаточных сведений по практической реализации). После получения конкретных параметров настройки, которые могут быть внедрены в состав проектируемой СЗИ, данные параметры включаются в итоговый перечень.

6. Дополнительно может осуществляться выбор мер детектирования (обнаружения) активности злоумышленника, реализующего технику. В качестве источника правил обнаружения может использоваться репозиторий аналитик обнаружения, также разработанный компанией MITRE – Cyber Analytic Repository (CAR) [16].

7. Проделанные этапы необходимо провести поочередно для всех мер защиты информации.

Далее рассмотрим пример применения предлагаемого подхода, продемонстрированный на рис. 2.

Пример иллюстрирует следующий порядок действий для каждого этапа подхода:

1. (1 этап) Рассматривается ИС, в отношении которой определен третий класс защищенности (для ИС, классифицированной в соответствии с документом [4]). Выбраны меры защиты ИАФ.1, ИАФ.4, УПД.1.

2. (2 этап) К выбранным мерам предъяв-

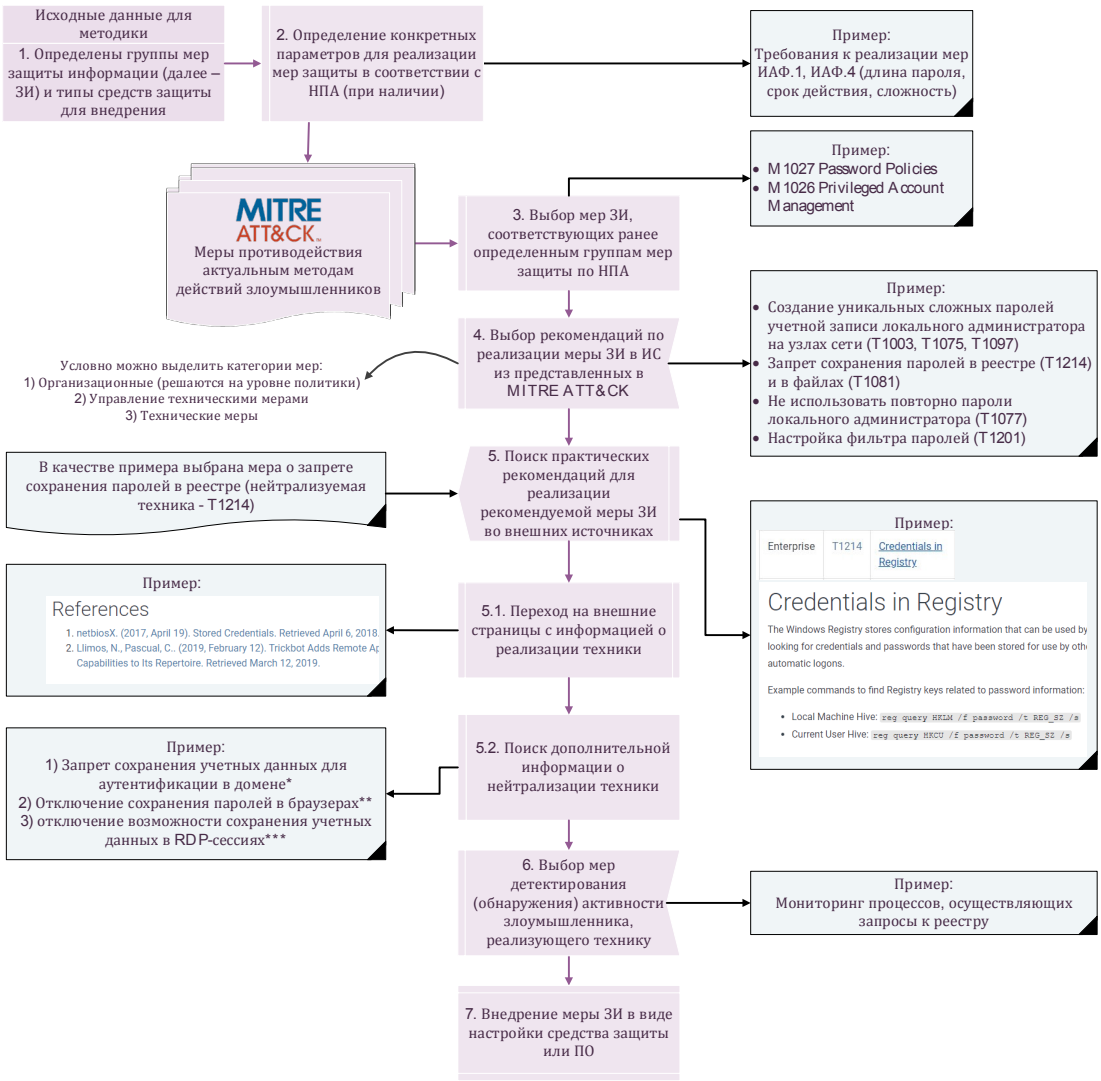

Рис. 2. Пример работы по предлагаемому подходу

ляются следующие требования для установленного класса защищенности: длина пароля должна составлять не менее 6 символов, алфавит пароля не менее 60 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут, срок действия пароля должен составлять не более 120 суток [8].

3. (3 этап) Наиболее подходящими категориями мер противодействия на странице Mitigations являются M1027 Password Policies (парольная политика) и M1026 Privileged Account Management (управление привилегированными пользователями).

Примечание: в примере рассматривается только несколько категорий мер противодействия из общего состава сопоставимых мер.

4. (4 этап) Для категорий M1026 и M1027 были выбраны следующие рекомендации по реализации мер противодействия:

– создание уникальных сложных паролей учетной записи локального администратора на узлах сети (T1003, T1075, T1097);

– запрет сохранения паролей в реестре (T1214) и в файлах (T1081);

– запрет повторного использования пароля локального администратора (T1077);

– настройка фильтра паролей (T1201).

Для дальнейшей демонстрации примера выбрана одна мера из перечисленных выше – запрет сохранения паролей в реестре (нейтрализуемая техника T1214).

5. (5 этап) Изучены сведения о технике действий злоумышленника T1214 Credentials in Registry. Суть реализации техники заключается в возможности осуществления запросов к реестру для перечисления учетных данных, хранимых в нем. После выполнения техники будет отображен любой раздел реестра, содержащий слово «пароль». В результате поиска дополнительной информации были определены рекомендуемые действия для фактической реализации меры защиты:

– настройка сохранения паролей ОС для аутентификации в домене [17];

– не разрешать хранение паролей или учетных данных для сетевой проверки подлинности в RDP-сессиях в соответствии с [18] и [19];

– блокировка сохранения паролей в браузерах на уровне групповых политик домена, например, [20] и [21].

6. (6 этап) Для рассматриваемой техники действий злоумышленника T1214 Credentials in Registry рекомендуется внедрить мониторинг приложений, которые могут быть использованы для запросов к реестру, например, Reg. Также рекомендуется сбор параметров команд, которые могут указывать на поиск учетных данных. В качестве источника для создания правил в SIEM-системе предлагается использовать репозиторий аналитик безопасности CAR [16]. Аналитики содержат в себе описание правил для внедрения в системы управления событиями безопасности и способы их тестирования [22].

7. Проделанные этапы повторяются для всех остальных мер защиты. Кроме того, необходимо учесть, что не все меры на этапе 4 были включены в настоящий пример и они также должны быть проработаны с учетом структурно-функциональных характеристик ИС.

6. Тестирование предлагаемого подхода интеграции знаний о мерах противодействия техникам современных компьютерных атак в существующий процесс проектирования системы защиты.

Для оценки качественных изменений в составе и содержании параметров настройки применим предлагаемый подход к примеру, из табл. 1.

Результаты проделанной работы представлены в табл. 4.

В табл. 4 рекомендации по конфигурированию системы защиты приведены не в полном объеме, но в составе достаточном для демонстрации результатов и составления выводов о применимости предлагаемого подхода. Приведенные рекомендации по конфигурированию указаны преимущественно для ОС Windows. При этом из состава Enterprise Mitigations также могут быть определены меры противодействия техникам для ОС семейства Linux.

Основная сложность при внедрении предлагаемого подхода заключается в необходимости поиска дополнительных сведений о практической реализации мер противодействия техникам действий злоумышленников. Однако формат ресурса ATT&CK требует определенного уровня универсальности приводимых в нем рекомендаций по предотвращению КА, что обуславливает высокоуровневость большинства мер противодействия.

7. Оценка эффективности принятых мер защиты, направленных на противодействие реализации современных угроз безопасности.

По результатам интеграции знаний о мерах противодействия техникам действий злоумышленников в процесс проектирования СЗИ необходимо определить дальнейшие действия по оценке эффективности принятых мер защиты против реализации УБИ. В частности, в ходе работы будут определены конкретные техники, блокирование которых

Таблица 4

Изменения в составе параметров конфигурирования по результатам интеграции предлагаемого подхода

№ п/п	Меры защиты	Параметры конфигурирования, принятые до интеграции знаний о мерах противодействия	Рекомендуемые дополнительные параметры конфигурирования для внедрения	Рекомендуемые дополнительные организационные меры	Нейтрализуемые УБИ и техники действий злоумышленников
1	ИАФ.1, ИАФ.3, ИАФ.4	– Максимальный период неактивности до блокировки экрана: 15 минут; – Количество неудачных попыток аутентификации: от 3 до 10 попыток; – Минимальная длина: не менее 6-8 символов; – Требования к сложности пароля: наличие строчных, прописных букв, цифр и символов – Срок действия пароля: не более 180/120/90/60 дней	– Двукратный сброс пароля учетной записи KRBTGT для деактивации билетов Kerberos (M1015) – Установка сложных паролей длиной более 25 символов для системных учетных записей (M1027); – Включение компонента Windows Defender Credential Guard в Windows 10 (M1043) – Ограничить число учетных записей, для которых разрешено кеширование паролей через параметр HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\cachedlogonscountvalue (M1028) – Настройка через GPO: Computer Configuration > [Policies] > Administrative Templates > SCM: Pass the Hash Mitigations: Apply UAC restrictions to local accounts on network logons (M1028) – не разрешать хранение паролей или учетных данных для сетевой проверки подлинности в RDP-сессиях (M1027) – блокировка сохранения паролей в браузерах на уровне групповых политик домена (M1027)	– Создание сложных и уникальных паролей, использование разных паролей на учетных записях локального администратора (M1027) – Создание различных учетных записей для администрирования и иных задач в ИС (M1027) – Запрет хранения паролей в файлах (M1027) – Установление требования по смене паролей по умолчанию при установке нового оборудования или ПО (M1027)	– УБИ.008 Угроза восстановления аутентификационной информации – УБИ.100 Угроза обхода некорректно настроенных механизмов аутентификации – T1003.005 OS Credential Dumping: Cached Domain Credentials – T1550.002 Use Alternate Authentication Material: Pass the Hash – T1021.002 Remote Services: SMB/Windows Admin Shares – T1558 Steal or Forge Kerberos Tickets T1552 Unsecured Credentials – T1547.008 Boot or Logon Autostart Execution: LSASS Driver

Окончание таблицы 4

2	УПД.2, УПД.4, УПД.5	– Контроль отсутствия административных прав у учетных записей пользователей на уровне системного и прикладного ПО – Назначение необходимых прав на файлы и каталоги, – Назначение необходимых прав в прикладном ПО для обеспечения выполнения трудовых обязанностей	– Замена учетной записи SYSTEM при создании задач, запускаемых по расписанию, на авторизуемую учетную запись через GPO или ключ реестра расположенный по пути HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl (M1026) – Запрет входа по RDP для учетной записи локального администратора (M1026) – Настройка фильтров WMI и групп безопасности для ограничения возможности изменения параметров GPO только отдельными учетными записями администраторов (M1026) – Ограничить права на создание logon-скриптов, разрешить только для тех учетных записей администраторов, которым эта функция необходима (M1022) – Задать максимальное время в течение которого может быть активна RDP-сессия и таймауты для проверки состояния (M1028)	– Переодический контроль состава назначенных прав у доменных и локальных учетных записей с целью выявления несанкционированных изменений (M1026)	– УБИ.006 Угроза внедрения кода или данных – УБИ.028 Угроза использования альтернативных путей доступа к ресурсам – T1053 Scheduled Task/Job – T1021.001 Remote Services: Remote Desktop Protocol – T1484 Domain Policy Modification – T1037 Boot or Logon Initialization Scripts – T1563.002 Remote Service Session Hijacking: RDP Hijacking
3	ОПС.1, ОПС.2	Настройка защищенной программной среды: – Прикладное ПО и его компоненты, которым разрешен запуск (например, Microsoft Office и средства чтения pdf документов в пользовательском сегменте, СУБД Postgree SQL, веб-сервер Nginx, docker-контейнеры в серверном сегменте) – Запрет запуска исполняемых файлов .exe и скриптов (.bat, PowerShell)	– В настройках application control запретить возможность запуска двоичных файлов, которые могут быть использованы злоумышленником и их функционирование в ИС не требуется (например, hh.exe, .cpl, CMSTP.exe, InstallUtil.exe, mshta.exe, Odbcconf.exe, Regasm.exe, verclsid.exe, msxsl.exe) (M1038)	–	– УБИ.178 Угроза несанкционированного использования системных и сетевых утилит – УБИ.188 Угроза подмены программного обеспечения – T1218 Signed Binary Proxy Execution – T1220 XSL Script Processing

должно быть обеспечено выбранными конфигурациями системного и прикладного ПО, а также СрЗИ.

В решении задачи оценки эффективности принятых мер защиты может быть применен метод эмуляции активности злоумышленника (adversary emulation), суть которого заключается в попытке успешно реализовать последовательность актуальных для защищаемой инфраструктуры техник из состава ATT&CK.

В качестве программного инструмента для эмуляции можно использовать набор тестов Atomic Red Team [23], который представляет собой свободно-распространяемый ресурс, в котором разработчики своевременно отражают изменения, происходящие в ATT&CK.

Тесты Atomic Red Team содержат в себе инструкции по реализации большинства техник действий злоумышленников. При работе с тестами может потребоваться корректировка приведенных инструкций в связи с возможной разницей в версиях программного обеспечения. Например, в разных версиях PowerShell потребуется использовать разный синтаксис команд.

В качестве примера осуществим эмуляцию техники T1550.002 Use Alternate Authentication Material: Pass the Hash. Суть техники заключается в том, что с помощью хэша пароля злоумышленник может действовать в скомпрометированной системе как будто обладает полными учетными данными [24].

Необходимо скачать и запустить утилиту Mimikatz [25] с использованием хэша пароля доменного администратора, который может быть получен путем реализации техники T1003 OS Credential Dumping. В результате будет запущена командная строка с правами администратора, что дает злоумышленнику неограниченные права в системе (рис. 3).

Утилита Mimikatz имеет широкий функционал и соответственно с применением техники Pass The Hash злоумышленником могут быть достигнуты и другие результаты.

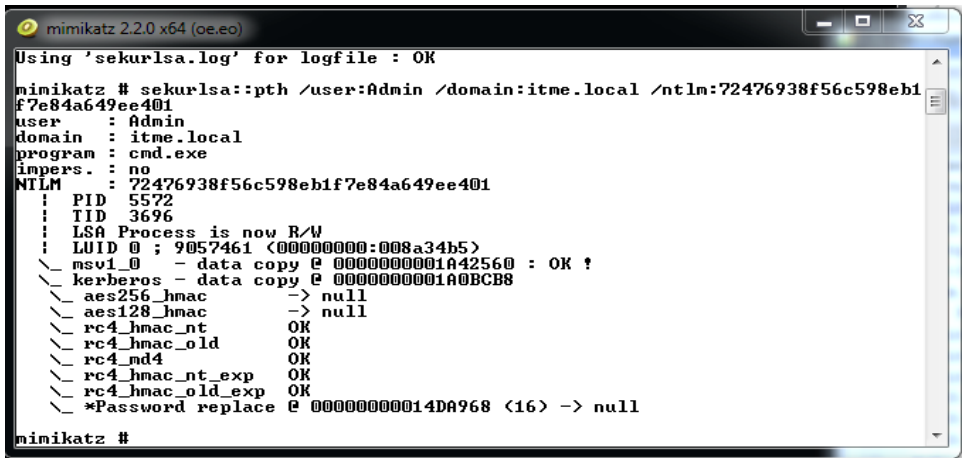

Рис. 3. Эмуляция техники с применением утилиты Mimikatz

Рекомендуемые параметры конфигурирования ИС для противодействия обозначенным техникам частично приведены в таблице 4. При этом необходимо учитывать, что рекомендации в составе ATT&CK Enterprise Mitigations не могут в ряде случаев обеспечить полную блокировку техники, но скорее направлены за увеличение времени и сложности в ее реализации злоумышленником. Это связано, как правило, с особенностями реализации архитектуры операционных систем, в которых многие функции не могут быть полностью отключены или перенастроены так чтобы реализация техники стала невозможна.

Тем не менее, предложенные к внедрению конфигурации выполняют целевую задачу по противодействию техникам действий злоумышленников и рекомендуются для интеграции в состав проектируемой системы защиты.

В результате интеграции знаний о мерах противодействия техникам действий злоумышленников специалистам предоставляется не только возможность выбора безопасных конфигураций для предотвращения реализации УБИ, но также механизм и инструменты для оценки реальной практической защищенности от них.

8. Заключение

Таким образом, в рамках работы был представлен подход по интеграции знаний о мерах противодействия КА в существующий процесс проектирования СЗИ, направленный на нейтрализацию УБИ и, в частности, техник действий злоумышленников через которые эти угрозы могут быть реализованы.

Предлагаемый подход развивает вопрос интеграции знаний о техниках КА, основывающийся на новой методике оценки УБИ, утвержденной ФСТЭК России [10].

Поэтому предлагаемый в рамках настоящей работы подход является одним из этапов развивающегося в России комплексного процесса защиты информации, выстраиваемого с учетом систематизированных и широко применяемых знаний о тактиках и техниках действий злоумышленников.

Литература

1. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Постановлением Госстандарта России от 30 июня 2000 г. 175-ст. – М.: Стандартинформ, 2022. – Текст: непосредственный.

2. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы: межгосударственный стандарт: издание официальное: утвержден и введен в действие Постановлением Государственного комитета СССР по стандартам от 24.03.89 № 661. – М.: Стандартинформ, 2022. – Текст: непосредственный.

3. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 января 2014 г. № 3-ст. – М.: Стандартинформ, 2022. – Текст: непосредственный.

4. Российская Федерация. Законы. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11.02.2013 № 17. –URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 14.09.2022). – Текст: электронный.

5. Российская Федерация. Законы. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18.02.2013 № 21. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 14.09.2022). – Текст: электронный.

6. Российская Федерация. Законы. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 25.12.2017 № 239 – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 14.09.2022). – Текст: электронный.

7. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 г. № 822-ст. – М.: Стандартинформ, 2020. – Текст: непосредственный.

8. Российская Федерация. Законы. Методический документ Меры защиты информации в государственных информационных системах: утвержден ФСТЭК России 11.02.2014 – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument (дата обращения: 14.09.2022). – Текст: электронный.

9. Российская Федерация. Законы. Методический документ. Методика оценки угроз безопасности информации: утвержден ФСТЭК России 5.02.2021 – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2022-g (дата обращения: 16.09.2022). – Текст: электронный.

10. Center for Internet Security. CIS Benchmarks. – URL: https://www.cisecurity.org/cis-benchmarks/ (дата обращения: 12.09.2022). – Текст: электронный.

11. Банк данных угроз безопасности информации ФСТЭК России. – URL: https://bdu.fstec.ru/threat (дата обращения: 14.09.2022). – Текст: электронный.

12. MITRE CVE. – URL: https://cve.mitre.org/ (дата обращения: 15.09.2022). – Текст: электронный.

13. Australian Cyber Security Centre. View all publications. – URL: https://www.cyber.gov.au/acsc/view-all-content/publications (дата обращения: 12.09.2022). – Текст: электронный.

14. Australian Cyber Security Centre. Strategies to Mitigate Cyber Security Incidents – Mitigation Details. February 2017. – URL: https://www.cyber.gov.au/sites/default/files/2021-10/PROTECT%20-%20Strategies%20to%20Mitigate%20Cyber%20Security%20Incidents%20%E2%80%93%20Mitigation%20Details%20%28February%202017%29.pdf (дата обращения: 12.09.2022). – Текст: электронный.

15. MITRE ATT&CK. – URL: https://attack.mitre.org/ (дата обращения: 12.09.2022). – Текст: электронный.

16. Full Analytic List. – URL: https://car.MITRE.org/wiki/Full_Analytic_List (дата обращения: 16.09.2022). – Текст: электронный.

17. Network access: Do not allow storage of passwords and credentials for network authentication. – URL: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-storage-of-passwords-and-credentials-for-network-authentication (дата обращения: 16.09.2022). – Текст: электронный.

18. Passwords must not be saved in the Remote Desktop Client. – URL: https://www.stigviewer.com/stig/windows_10/2015-11-30/finding/V-63729 (дата обращения: 16.09.2022). – Текст: электронный.

19. Cached Credentials: Important Facts That You Cannot Miss. – URL: https://cqureacademy.com/blog/windows-internals/cached-credentials-important-facts (дата обращения: 16.09.2022). – Текст: электронный.

20. Disable Browser Password Saving via Group Policy. – URL: https://support.practiceprotect.com/knowledge-base/disable-browser-password-saving-via-group-policy/ (дата обращения: 16.09.2022). – Текст: электронный.

21. Disabling the option to save a password on Internet Explorer. – URL: https://searchsecurity.techtarget.com/answer/Disabling-the-option-to-save-a-password-on-Internet-Explorer (дата обращения: 16.09.2022). – Текст: электронный.

22. CAR-2013-03-001: Reg.exe called from Command Shell. – URL: https://car.MITRE.org/analytics/CAR-2013-03-001/ (дата обращения: 16.09.2022). – Текст: электронный.

23. Atomic-red-team. – URL: https://github.com/redcanaryco/atomic-red-team (дата обращения: 16.09.2022). – Текст: электронный.

24. T1550.002 – Pass the Hash. – URL: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1550.002/T1550.002.md (дата обращения: 16.09.2022). – Текст: электронный.

25. Mimikatz. – URL: https://github.com/gentilkiwi/mimikatz (дата обращения: 16.09.2022). – Текст: электронный.

References

1. GOST R 51624-2000. Zashchita informatsii. Avtomatizirovannyye si-stemy v zashchishchennom ispolnenii. Obshchiye trebovaniya: natsional'nyy stan-dart Rossiyskoy Federatsii: izdaniye ofitsial'noye: utverzhden i vveden v deystviye Postanovleniyem Gosstandarta Rossii ot 30 iyunya 2000 g. 175-st. – M.: Standartinform, 2022. – Tekst: neposredstvennyy.

2. GOST 34.602-89. Informatsionnaya tekhnologiya. Kompleks standar-tov na avtomatizirovannyye sistemy. Tekhnicheskoye zadaniye na sozdaniye avto-matizirovannoy sistemy: mezhgosudarstvennyy standart: izdaniye ofitsial'-noye: utverzhden i vveden v deystviye Postanovleniyem Gosudarstvennogo komi-teta SSSR po standartam ot 24.03.89 № 661. – M.: Standartinform, 2022. – Tekst: neposredstvennyy.

3. GOST R 51583-2014. Zashchita informatsii. Poryadok sozdaniya avto-matizirovannykh sistem v zashchishchennom ispolnenii. Obshchiye polozheniya: natsional'nyy standart Rossiyskoy Federatsii: izdaniye ofitsial'noye: utverzhden i vveden v deystviye Prikazom Federal'nogo agentstva po tekhnicheskomu regulirovaniyu i metrologii ot 28 yanvarya 2014 g. № 3-st. – M.: Standartinform, 2022. – Tekst: neposredstvennyy.

4. Rossiyskaya Federatsiya. Zakony. Ob utverzhdenii trebovaniy o za-shchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh: prikaz FSTEK Rossii ot 11.02.2013 № 17. –URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (data obrashcheniya: 14.09.2022). – Tekst: elektronnyy.

5. Rossiyskaya Federatsiya. Zakony. Ob utverzhdenii sostava i soderzha-niya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti per-sonal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh perso-nal'nykh dannykh: prikaz FSTEK Rossii ot 18.02.2013 № 21. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (data obrashcheniya: 14.09.2022). – Tekst: elektronnyy.

6. Rossiyskaya Federatsiya. Zakony. Ob utverzhdenii Trebovaniy po obespecheniyu bezopasnosti znachimykh ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: prikaz FSTEK Rossii ot 25.12.2017 № 239 – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (data obrashcheniya: 14.09.2022). – Tekst: elektronnyy.

7. GOST R 57580.1-2017. Bezopasnost' finansovykh (bankovskikh) ope-ratsiy. Zashchita informatsii finansovykh organizatsiy. Bazovyy sostav orga-nizatsionnykh i tekhnicheskikh mer: natsional'nyy standart Rossiyskoy Fede-ratsii: izdaniye ofitsial'noye: utverzhden i vveden v deystviye Prikazom Fe-deral'nogo agentstva po tekhnicheskomu regulirovaniyu i metrologii ot 08.08.2017 g. № 822-st. – M.: Standartinform, 2020. – Tekst: neposred-stvennyy.

8. Rossiyskaya Federatsiya. Zakony. Metodicheskiy dokument Mery za-shchity informatsii v gosudarstvennykh informatsionnykh sistemakh: utverzhden FSTEK Rossii 11.02.2014 – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument (data obrashcheniya: 14.09.2022). – Tekst: elektronnyy.

9. Rossiyskaya Federatsiya. Zakony. Metodicheskiy dokument. Metodika otsenki ugroz bezopasnosti informatsii: utverzhden FSTEK Rossii 5.02.2021 – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2022-g (data obra-shcheniya: 16.09.2022). – Tekst: elektronnyy.

10. Center for Internet Security. CIS Benchmarks, available at: https://www.cisecurity.org/cis-benchmarks/ (accessed: 12.09.2022).

11. Bank dannykh ugroz bezopasnosti informatsii FSTEK Rossii. – URL: https://bdu.fstec.ru/threat (data obrashcheniya: 14.09.2022). – Tekst: elek-tronnyy.

12. MITRE CVE, available at: https://cve.mitre.org/ (accessed: 15.09.2022).

13. Australian Cyber Security Centre. View all publications, available at: https://www.cyber.gov.au/acsc/view-all-content/publications (accessed: 12.09.2022).

14. Australian Cyber Security Centre. Strategies to Mitigate Cyber Security Incidents – Mitigation Details. February 2017, available at: https://www.cyber.gov.au/sites/default/files/2021-10/PROTECT%20-%20Strategies%20to%20Mitigate%20Cyber%20Security%20Incidents%20%E2%80%93%20Mitigation%20Details%20%28February%202017%29.pdf (accessed: 12.09.2022).

15. MITRE ATT&CK, available at: https://attack.mitre.org/ (accessed: 12.09.2022).

16. Full Analytic List, available at: https://car.MITRE.org/wiki/Full_Analytic_List (accessed: 16.09.2022).

17. Network access: Do not allow storage of passwords and credentials for network authentication, available at: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-storage-of-passwords-and-credentials-for-network-authentication (accessed: 16.09.2022).

18. Passwords must not be saved in the Remote Desktop Client, available at: https://www.stigviewer.com/stig/windows_10/2015-11-30/finding/V-63729 (accessed: 16.09.2022).

19. Cached Credentials: Important Facts That You Cannot Miss, available at: https://cqureacademy.com/blog/windows-internals/cached-credentials-important-facts (accessed: 16.09.2022).

20. Disable Browser Password Saving via Group Policy, available at: https://support.practiceprotect.com/knowledge-base/disable-browser-password-saving-via-group-policy/ (accessed: 16.09.2022).

21. Disabling the option to save a password on Internet Explorer, available at: https://searchsecurity.techtarget.com/answer/Disabling-the-option-to-save-a-password-on-Internet-Explorer (accessed: 16.09.2022).

22. CAR-2013-03-001: Reg.exe called from Command Shell, available at: https://car.MITRE.org/analytics/CAR-2013-03-001/ (accessed: 16.09.2022).

23. Atomic-red-team, available at: https://github.com/redcanaryco/atomic-red-team (accessed: 16.09.2022).

24. T1550.002 – Pass the Hash, available at: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1550.002/T1550.002.md (accessed: 16.09.2022).

25. Mimikatz, available at: https://github.com/gentilkiwi/mimikatz (accessed: 16.09.2022).

ГОЛУШКО Анна Павловна, аспирант, кафедра безопасности информационных технологий, ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева». Россия, 660037, Красноярский край, г. Красноярск, пр. имени газеты «Красноярский рабочий», д. 31. E-mail: golushko.ap@yandex.ru

ЖУКОВ Вадим Геннадьевич, кандидат технических наук, доцент кафедры безопасности информационных технологий, ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева». Россия, 660037, Красноярский край, г. Красноярск, пр. имени газеты «Красноярский рабочий», д. 31. E-mail: zhukov@sibsau.ru

GOLUSHKO Anna Pavlovna, Postgraduate student, Information Technologies Security Department, Reshetnev Siberian State University of Science and Technology. 660037, Krasnoyarsk Territory, Krasnoyarsk, avenue named after the newspaper "Krasnoyarsky Rabochiy", 31. E-mail: golushko.ap@yandex.ru.

ZHUKOV Vadim Gennadievich, Candidate of Technical Sciences, Associate Professor of the Department of Information Technology Security, Reshetnev Siberian State University of Science and Technology. 660037, Krasnoyarsk Territory, Krasnoyarsk, avenue named after the newspaper "Krasnoyarsky Rabochiy", 31. E-mail: zhukov@sibsau.ru