УДК *004.056*

А. О. Махнев, Н. П. Деканова

Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

ИССЛЕДОВАНИЕ ПЛАТФОРМ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *Платформы управления инцидентами помогают администраторам, ответственным за информационную безопасность оперативно выявлять и расследовать инциденты, управлять своей работой до момента его закрытия и автоматизировать задачи реагирования на инциденты для обеспечения более быстрого проведения работ с выявленными происшествиями.*

Управление инцидентами - это сложная технология, требующая квалифицированных ИТ-инженеров и аналитиков для управления и поддержки. Внедряя систему необходимо понимать, что она не является универсальным средством для устранения всех атак и инцидентов, связанных с информационной безопасностью.

Ключевые слова: *информационная безопасность, платформа реагирования на инциденты, инцидент информационной безопасности, событие информационной безопасности.*

A.O. Mahnev, N.P. Dekanova

Irkutsk State Transport University, Irkutsk, the Russian Federation

INVESTIGATION OF INFORMATION SECURITY INCIDENTS RESPONSE PLATFORMS

Abstract. *Incident management platforms help security administrators quickly identify and investigate incidents, manage their work until the point of closure, and automate incident response tasks to ensure faster resolution of identified incidents.*

Incident management is a complex technology that requires skilled IT engineers and analysts to manage and support. When implementing a system, you need to understand that it is not a universal remedy for eliminating all attacks and incidents related to information security.

Keywords: *information security, incident response platform, information security incidents, information security event.*

Современное состояние и развитие систем обеспечения информационной безопасности как в России, так и за рубежом характеризуются стремлением автоматизировать процессы реагирования на все возрастающее разнообразие инцидентов информационной безопасности. Причем на критические инциденты необходимо реагировать в считанные минуты. В связи с этим изучение процессов и задач реагирования на инциденты информационной безопасности является актуальным направлением исследований.

Цель данного исследования заключается в обзорном анализе систем автоматизации процессов реагирования на инциденты информационной безопасности. Система защиты от утечек информации состоит из обнаружения, предотвращения, реагирования и регистрации инцидента, а также включает устранение последствий инцидентов информационной безопасности или событий, нарушающих установленные процедуры защиты информационной безопасности (ИБ).

В соответствии со стандартом Российской Федерации от 01.07.2008 года ГОСТ Р ISO/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Information technology. Security techniques. Information security incident management» (далее – Стандарт менеджмента инцидентов) инцидент информационной безопасности (information security incident) – появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ. Понятие инцидента тесно связано с таким понятием как событие

информационной безопасности. Согласно Стандарта событие информационной безопасности (information security event) – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности [1]. Любые отклонения в защищаемых информационных ресурсах могут рассматриваться как события информационной безопасности. Каждое событие должно быть оценено с точки зрения того, является ли это событие инцидентом информационной безопасности.

На сегодняшний день количество инцидентов ИБ, особенно в крупных организациях, достаточно велико и продолжает расти с каждым годом. Согласно данным компании Positive Technologies количество инцидентов в области информационной безопасности в 2021 году увеличилось на 6,5 % по сравнению с 2020 годом. Как и в 2020 году, 86 % всех атак направлены на организации. Больше всего злоумышленников интересовали государственные и медицинские учреждения, а также промышленные компании [2]. На рисунках 1, 2 представлены статистические данные.

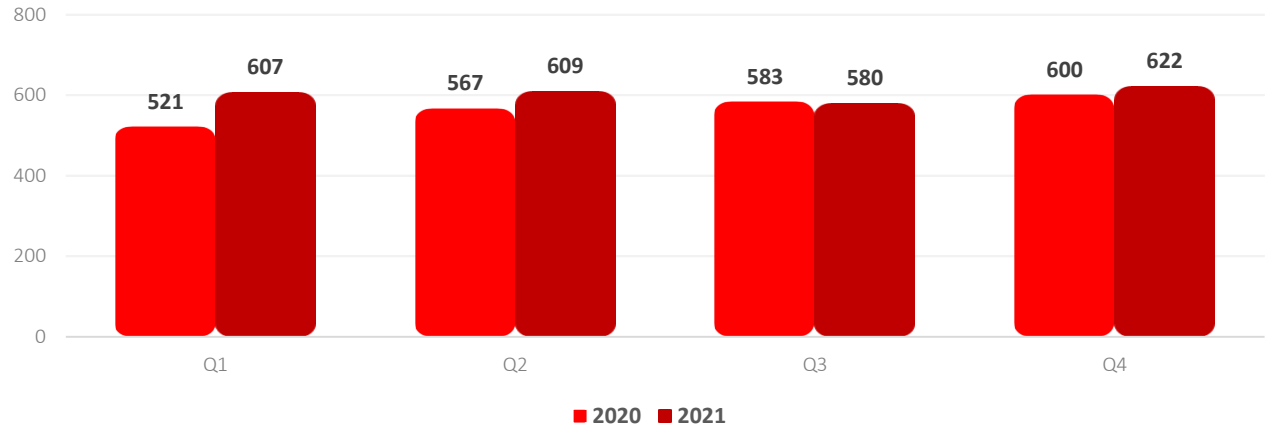

Рис. 1 – Количество инцидентов в 2000 и 2021 годах

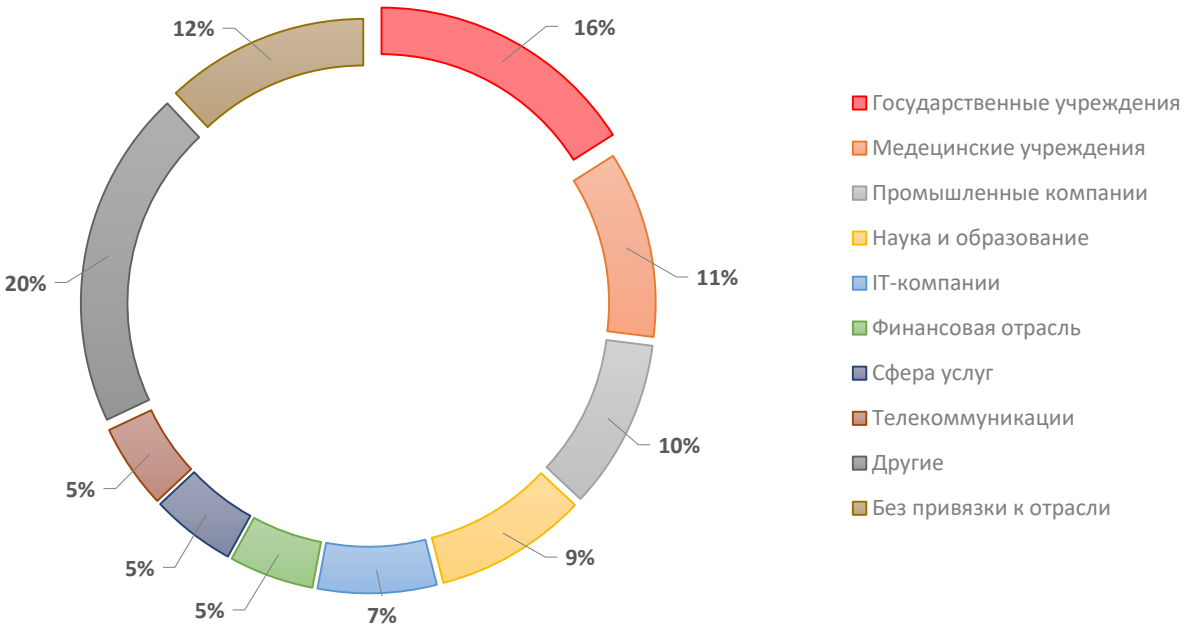

Рис. 2– Категории организаций, ставших жертвами атак

С целью автоматизации процессов реагирования на инциденты разработана платформа Incident Response Platform (далее – IRP) – система автоматизации реагирования на инциденты информационной безопасности. Система IRP помогает выполнить заданный алгоритм операций согласно внутреннему регламенту реагирования на инциденты ИБ по сбору дополнительной информации, осуществить неотложные действия по сдерживанию и устранению угрозы, восстановить атакованную систему, оповестить заинтересованных лиц, а также собрать и структурировать данные о расследованных инцидентах информационной безопасности. Кроме того, система IRP позволяет роботизировать и автоматизировать однотипные действия оператора-специалиста ИБ, которые он производит при реагировании на инциденты информационной безопасности, что помогает снизить нагрузку сотрудника в части выполнения рутинных операций.

Программное обеспечение управления инцидентами автоматизирует процесс и предоставляет пользователям инструменты, необходимые для поиска и устранения нарушений безопасности. Компании используют инструменты для мониторинга сетей, инфраструктуры и конечных точек на предмет вторжений и аномальной активности. Затем они используют программы для проверки и устранения вторжений и вредоносных программ в системе. Эти продукты предоставляют возможности для решения проблем, возникающих после того, как угрозы минуют брандмауэры и другие механизмы безопасности. Они предупреждают администраторов о несанкционированном доступе к приложениям и сетям [3].

Присутствие системы управления инцидентами в организации может снизить стоимость последствий от нарушения информационной безопасности, сэкономив организации суммы на восстановление информационных активов и потерю репутации.

Преимущества наличия системы управления инцидентами в организации:

- базовый мониторинг безопасности;
- обнаружение инцидентов безопасности;
- уведомления и предупреждения в режиме реального времени;
- оптимизированные операции;
- интеграция со сторонними приложениями;
- облачное или локальное развертывание.

На рисунке 3 приведен пример функциональности систем управления инцидентами информационной безопасностью.

Рис. 3 – Структурная схема процессов реагирования на инцидент

Jet Signal – собственное программное решение компании «Инфосистемы Джет», предназначенное для повышения эффективности обработки инцидентов информационной безопасности. Решение дает возможность службам ИБ работать в едином информационном пространстве: расследовать инциденты, назначать поручения и контролировать их исполнение, использовать накопленный опыт в базе знаний, общаться во встроенном чате.

Гибкая архитектура системы Jet Signal позволяет оперативно адаптировать решение к изменениям на рынке и потребностям пользователей. Решение предназначено для предприятий любых сфер деятельности, в том числе, обладающих территориально-распределенной инфраструктурой. Может применяться для обработки информации разной степени конфиденциальности с возможностью односторонней связи между контурами защиты. На систему Jet Signal имеются свидетельство о государственной регистрации программы для ЭВМ № 2017612966 и сертификат соответствия требованиям безопасности информации по уровню контроля 2 НДВ и РДВ системы сертификации Министерства обороны РФ № 3712 [4].

Security Vision IRP – программный продукт для автоматизации действий по управлению информационной безопасностью и реагированию на инциденты кибербезопасности. [5]. Система обеспечивает:

- автоматическое выполнение дежурных процедур в режиме реального времени;
- снижение воздействия инцидентов кибербезопасности за счет снижения времени реагирования на инциденты в вопросах: идентификации, локализации, уничтожения и восстановления;
- снижение риска человеческого фактора и ошибок персонала, привлекаемого на реагирование инцидентов кибербезопасности;
- сокращение времени реагирования за счет автоматизации набора заранее разработанных процедур и сценариев реагирования, реализованных в компонентах Системы.

Выданный ФСТЭК России Сертификат соответствия № 4194 от 19.12.19 удостоверяет, что Security Vision полностью соответствует нормам действующих нормативных-правовых актов Российской Федерации (в частности, по 4-му уровню контроля отсутствия недекларированных возможностей), и подтверждает высокий уровень защиты информации, обрабатываемой в Security Vision.

R-Vision Incident Response Platform (далее – R-Vision IRP) представляет собой автоматизированный центр мониторинга, обработки и реагирования на инциденты информационной безопасности [6]. Платформа R-Vision IRP позволяет выявлять киберугрозы и инциденты в режиме реального времени, собирая информацию из множества источников в едином окне оперативного реагирования. При обнаружении инцидента запускаются преднастроенные алгоритмы и автоматизированные сценарии, которые обеспечивают быстроту реакции и слаженность действий команды реагирования, помогая свести к минимуму возможные негативные последствия от инцидента.

Для отслеживания эффективности обеспечения информационной безопасности и отдельных процессов предусмотрен широкий набор метрик и средств визуализации. Готовые шаблоны сводок позволяют быстро формировать отчетность для руководства, регуляторов и внутренних пользователей и отправлять ее адресатам в автоматическом режиме. R-Vision IRP предлагает набор возможностей по автоматизации реагирования, которые могут быть легко настроены пользователем системы под собственные нужды.

Сценарии реагирования позволяют в автоматическом режиме реализовать алгоритм действий, заданный для конкретного типа инцидента при срабатывании определенного правила. Например, в сценарий реагирования могут быть включены такие действия как:

- постановка задач, отправка уведомлений, принятие решений;
- действия, направленные на блокировку атаки и минимизацию возможных последствий;
- сбор ключевой информации для расследования инцидента, отправка запросов, запрос событий по инциденту в SIEM;

- запуск необходимых коннекторов и сценариев реагирования.

Для быстрого старта в системе предусмотрен набор типовых сценариев реагирования, а встроенный графический редактор позволяет их легко адаптировать под специфику организации и конкретную структуру команды реагирования. Скрипты автоматизации позволяют удаленно осуществлять сбор данных и выполнять определенные действия на оборудовании. В системе представлено более 50 готовых скриптов и их список постоянно пополняется. Имеется возможность создавать собственные скрипты на любом скриптовом языке. Карта рабочего процесса по инциденту позволяет быстро оценить статус обработки инцидента, увидеть, сколько шагов выполнено, какие действия выполняются в данный момент и внести изменения на лету.

Программный комплекс обеспечивает проведение инвентаризации инфраструктуры, выделение наиболее критичных активов, определение специалистов, ответственных за безопасность активов. За счет интеграции с имеющимися решениями по безопасности (антивирусы, сканеры защищенности и др.), а также использования собственных механизмов контроля, обеспечиваются:

- консолидация и представление в единой консоли различных сведений о состоянии безопасности инфраструктуры,
- контроль установленного ПО,
- обнаружение несанкционированного оборудования и внешних подключений,
- выявление и контроль устранения уязвимостей.

Топология инфраструктуры может быть представлена в виде карт сетей, планов помещений и схем географического расположения. Сбор и консолидация необходимой информации по состоянию ИТ-инфраструктуры и зафиксированным инцидентам информационной безопасности могут быть обеспечены за счет использования нескольких механизмов:

- электронной почты,
- программного интерфейса (API),
- встроенной системы приема сообщений
- собственных коннекторов для ключевых систем защиты: сканеров уязвимости, средств антивирусной защиты, систем защиты от утечки информации (DLP), систем сбора и корреляции событий безопасности (SIEM) и других.

Разбор поступающих в систему сообщений может быть адаптирован под специфику защищаемой инфраструктуры путем использования правил на базе регулярных выражений или тегов. Отсутствие единого центра, содержащего сведения обо всех зафиксированных инцидентах информационной безопасности, является одной их ключевых проблем, снижающих оперативность реагирования на инциденты уполномоченных сотрудников. Использование платформы IRP в качестве основы для реализации центра реагирования на инциденты ИБ (SOC) позволяет обеспечить фиксацию фактов обнаружения инцидентов информационной безопасности, а также релевантной информации в единой, централизованной базе. Это, в свою очередь, позволяет повысить управляемость деятельности по реагированию на инциденты и оперативность обработки возникающих инцидентов, а также соблюсти соответствующие требования методических документов и стандартов, установленных регуляторами. Платформа IRP содержит широкий спектр механизмов, позволяющих адаптировать логику работы системы под специфику и особенности процесса реагирования на инциденты в определенной компании. К таким механизмам относятся:

- конструктор описания инцидентов, позволяющий задать состав сведений, собираемых по соответствующим категориям инцидентов;
- конструктор циклов обработки инцидентов, позволяющий создавать различные схемы статусов (маршруты) движения инцидентов в процессе обработки;
- гибкие правила настройки доступа к сведениям по инцидентам, включая возможность автоматического назначения ответственных лиц на инциденты на основании связанных активов, или заданных правил;

- настраиваемые справочники и шаблоны инцидентов, обеспечивающие возможность быстрого ввода данных по зафиксированным инцидентам.

Платформа IRP предлагает широкий набор средств визуализации информации. Кастомизируемые дашборды обеспечивают представление информации в виде графиков и диаграмм, содержащих функции перехода от графиков к соответствующей им информации. Данные по инфраструктуре могут быть представлены в виде карт сетей и схем помещений. Анализ взаимосвязей между элементами системы, способствующий эффективному расследованию инцидентов, может быть проведен с использованием так называемых схем взаимосвязей. Информация по активам, инцидентам и другим элементам системы для ее последующей обработки также может быть экспортирована в виде Excel-файлов. R-Vision IRP содержит широкий список готовых отчетов, а также механизмы настройки собственных шаблонов. Правила создания и рассылки отчетов позволяют настроить расписание автоматической генерации документов и их отправки соответствующим адресатам.

Программное обеспечение включено в единый реестр российских программ для электронных вычислительных машин и баз данных, рег.номер: 1954. Компания R-Vision получила сертификат Федеральной службы по техническому и экспортному контролю (ФСТЭК) России по 4-му уровню доверия на программный комплекс «Центр контроля информационной безопасности Р-Вижн» (далее – ЦКИБ Р-Вижн). Выданный ведомством сертификат № 4346 действует до 22 декабря 2025 года. Он подтверждает возможность использовать платформы R-Vision IRP и R-Vision SGRC, входящие в состав ЦКИБ Р-Вижн, в значимых объектах критической информационной инфраструктуры (КИИ) 1 категории и автоматизированных системах управления производственными и технологическими процессами (АСУ ТП) 1 класса защищенности. Также данный программный комплекс можно применять в государственных информационных системах (ГИС) 1 класса защищенности, в информационных системах персональных данных (ИСПДн) при необходимости обеспечения 1 уровня защищенности персональных данных и в информационных системах общего пользования II класса.

Разработка алгоритмов сценариев реагирования на инциденты информационной безопасности для конкретного типа инцидента позволяет автоматизировать процессы при срабатывании определенного правила [7]. На базе платформы R-Vision IRP рассмотрим алгоритм сценария реагирования на инцидент информационной безопасности типа «Несанкционированный доступ к личному кабинету». Инцидент заключается в обращении пользователя о несанкционированном доступе к сервису «Личный кабинет пользователя» (далее – Сервис) или компрометации аутентификационной информации, используемой для доступа к Сервису, а также поступление иной информации, свидетельствующей о доступе третьих лиц к Сервису. Инцидент имеет категорию «критичный» и относится к виду: компьютерная атака на компоненты информационных систем и иные действия, которые могут реализовывать уязвимости информационной системы. Формирование инцидента на платформе R-Vision IRP производится администратором информационной безопасности на основании сообщения от пользователя о несанкционированном доступе к Сервису или компрометации аутентификационной информации, используемой для доступа к Сервису как на основании документированного заявления гражданина, так и на основании иных обращений, а также поступление иной информации, свидетельствующей о доступе третьих лиц к Сервису. Администратор информационной безопасности назначает указанный инцидент соответствующему ответственному лицу за данный инцидент или проводит дальнейшие действия самостоятельно. После формирования инцидента платформа R-Vision IRP автоматически назначает указанный инцидент на сотрудника технической поддержки, который обеспечивает формирование сведений о событиях информационной безопасности, сформированных в подсистеме мониторинга действий пользователей в отношении пользователя, и прикладывает указанную информацию в карточку инцидента. Администратор информационной безопасности переводит карточку инцидента в статус «Расследование», и проводятся следующие мероприятия:

- получаются сведения о регистрационных действиях в Личном кабинете пользователя;
- инициирование блокировки (запрет на дальнейшую обработку информации, поданной через Сервис от имени пользователя);
- включение учетной записи пользователя и смена пароля при следующем входе;
- просмотр журналов событий учетной записи пользователя и их анализ ответственным исполнителем;
- инициирование служебного расследования и выявление причин возникновения инцидента информационной безопасности;
- заключение ответственного исполнителя на основании собранной информации;
- уведомление о закрытии инцидента рабочей группы.

На рисунке 4 представлен сценарий реагирования на инцидент информационной безопасности в информационной системе типа «Несанкционированный доступ к личному кабинету».

Рис. 4 Сценарий реагирования на инцидент типа «Несанкционированный доступ к личному кабинету»

Заключение. В статье представлены результаты обзорного анализа ряда систем автоматизации процессов реагирования на инциденты информационной безопасности. Рассмотренные платформы, сертифицированные в Российской Федерации, различаются алгоритмами выполнения операций по сдерживанию и устранению угрозы, восстановлению атакованной системы, оповещению заинтересованных лиц, а также сбору и структурированию данных о расследованных инцидентах информационной безопасности. Одной из наиболее перспективных для дальнейшего развития и модернизации является платформа управления инцидентами Incident Response Platform, в которой имеется возможность создавать собственные скрипты на любом скриптовом языке. Большинство задач, кроме тех, которые выполняются администратором информационной безопасности, могут быть автоматизированы в системе, и часть из них может выполняться параллельно. Управление инцидентами это сложная технология, требующая квалифицированных ИТ-инженеров и аналитиков для управления и поддержки. Внедряя или модернизируя систему необходимо понимать, что она не является универсальным средством для устранения всех атак и инцидентов, связанных с информационной безопасностью. Платформы управления инцидентами помогают администраторам, ответственным за информационную безопасность,

оперативно выявлять и расследовать инциденты, управлять работой системы до момента их закрытия и автоматизировать задачи реагирования на инциденты для обеспечения более быстрого проведения работ с выявленными происшествиями.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности [Электронный ресурс]. – URL http://docs.cntd.ru/document/1200068822 (07.05.2022).
2. Positive Technologies. Актуальные киберугрозы: итоги 2021 года [Электронный ресурс]. – URL https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/ (06.05.2022).
3. Бодрик А.П. Обзор рынка платформ реагирования на инциденты (IRP) в России. [Электронный ресурс]. – URL https://www.anti-malware.ru/analytics/Market_Analysis/incidentresponse-platforms -irp-in-russia/ (20.04.2022).
4. Jet. Система Jet Signal [Электронный ресурс]. – URL https://jet.su/services/software-development/products/jet-signal/ (06.05.2022).
5. Security Vision. Система Security Vision IRP [Электронный ресурс]. – URL https://www.securityvision.ru/products/irp/ (06.05.2022).
6. R-Vision. Система R-Vision Incident Response Platform [Электронный ресурс]. – URL https://rvision.pro/irp/ (06.05.2022).
7. Панасенко А. Автоматизация реагирования на инциденты с помощью сценариев (playbook) на примере R-Vision IRP [Электронный ресурс]. – URL https://www.anti-malware.ru/practice/methods/R-Vision-IRP (18.05.2022).

REFERENCES

1. ГОСТ Р ИСО/МЭК ТО 18044-2007. Information technology. Security techniques. Information security incident management [Electronic resource]. – URL http://docs.cntd.ru/document/1200068822 (07.05.2022).
2. Positive Technologies. Actual cyber threats: results of 2021 [Electronic resource]. – URL https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/ (06.05.2022).
3. Bodrik A.P. Market Overview of Incident Response Platforms (IRP) in Russia. [Electronic resource]. – URL https://www.anti-malware.ru/analytics/Market_Analysis/incidentresponse-platforms -irp-in-russia/ (20.04.2022).
4. Jet. Sysrem Jet Signal [Electronic resource]. – URL https://jet.su/services/software-development/products/jet-signal/ (06.05.2022).
5. Security Vision. Система Security Vision IRP [Electronic resource]. – URL https://www.securityvision.ru/products/irp/ (06.05.2022).
6. R-Vision. System R-Vision Incident Response Platform [Electronic resource]. – URL https://rvision.pro/irp/ (06.05.2022).
7. Panasenko A. Automating incident response using scripts (playbook) using the example of R-Vision IRP [Electronic resource]. – URL https://www.anti-malware.ru/practice/methods/R-Vision-IRP (18.05.2022).

Информация об авторах

Махнев Артем Олегович - аспирант кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: ib.38@mail.ru

Деканова Нина Петровна - д.т.н., профессор кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск e-mail: dekanova_np@irgups.ru

Information about the authors

Mahnev Artem Olegovich – postgraduate student of the department "Information systems and information protection", Irkutsk State Transport University, Irkutsk, e-mail: ib.38@mail.ru

Dekanova Nina Petrovna – Ph.D. in Engineering Science, Associate Professor of the Department "Information systems and information protection", Irkutsk State Transport University, Irkutsk, e-mail: dekanova_np@irgups.ru