УДК 004.056

Игошина Ю.В

Студент 4 курса, напр. «Экономическая безопасность»

ФГАОУ ВО Волгоградский государственный университет,

Россия, г. Волгоград

Научный Руководитель: Соколов П.С. доцент, к.э.н.

ФГАОУ ВО Волгоградский государственный университет

ОРГАНИЗАЦИЯ ЗАЩИТЫ УЧЕТНОЙ ИНФОРМАЦИИ В УСЛОВИЯХ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Аннотация: в статье рассматривается организация защиты учетной информации в условиях обеспечения кибербезопасности на примере ПАО «ГМК Норильский никель». Актуальность статьи обуславливается высоким развитием информационных технологий и появлением соответствующих проблем. Исследование проводилось путем изучения защиты учетной информации и анализа осуществления защиты учетной информации в условиях обеспечения кибербезопасности в ПАО «ГМК Норильский никель». В результате были сделаны положительные вывод о ПАО «ГМК Норильский никель».

Ключевые слова: кибербезопасность, учетная информация, организация защиты, угроза, информационная безопасность.

ORGANIZATION OF ACCOUNT INFORMATION PROTECTION IN THE CONTEXT OF CYBERSECURITY

Igoshina Yu.V.

4th year student, e.g. "Economic security"

Volgograd State University,

Russia, Volgograd

Scientific supervisor: Sokolov P.S. Associate Professor, Ph.D.

Volgograd State University

Abstract: the article discusses the organization of accounting information protection in the context of cybersecurity on the example of PJSC MMC Norilsk Nickel. The relevance of the article is due to the high development of information technology and the emergence of relevant problems. The study was conducted by studying the protection of accounting information and analyzing the implementation of accounting information protection in the

context of cybersecurity at PJSC MMC Norilsk Nickel. As a result, positive conclusions were made about PJSC MMC Norilsk Nickel.
Keywords: cybersecurity, accounting information, organization of protection, threat to information security, types of information.
Введение. В последние годы все больше становятся актуальными вопросы кибербезопасности, в связи с активным развитием информационных технологий. Вместе с информационными технологиями сопоставимо происходит рост кражи информации, нашествия кибератак, киберугроз и т.д. На основании этого выбранная тема имеет высокую актуальность для исследования. Исследование проводится на примере ПАО «ГМК Норильский никель». В данной работе для исследования были рассмотрены основные риски безопасности учетной информации меры и методы информационной безопасности благодаря чему можно было сделать вывод о состоянии учетной информации ПАО «ГМК Норильский никель».

Прежде чем изучать особенности организации защиты учетной информации в условиях кибербезопасности, рассмотрим перечень определений, непосредственно относящихся к данной теме:

1. Кибербезопасность – это область информационной безопасности, которая занимается защитой компьютерных систем, сетей, программного обеспечения и данных от киберугроз. Она включает в себя меры по предотвращению кибератак, обнаружению и реагированию на инциденты безопасности, а также обеспечение конфиденциальности, целостности и доступности информации.

2. Защита учетной информации – это исключение возможности как случайного, так и умышленного воздействия на нее, которое может привести к ущербу для владельцев или пользователей данных.

3. Информационная безопасность учетных данных в узком – это надежная работа компьютерной системы, сохранность ценных данных учета, защита информации от несанкционированных изменений, сохранение документированных учетных записей в электронные формы. В широком смысле – это обеспечение конфиденциальности, целостности и доступности информации, связанной с учетными данными пользователей, включающее в себя защиту логинов, паролей, персональных данных и другой конфиденциальной информации, которая используется для

идентификации и аутентификации пользователей в различных информационных системах.

4. Угроза информационной безопасности – это потенциальная возможность оказания воздействия на компоненты учетной системы, что может причинить вред владельцам информационных ресурсов или пользователям системы. В контексте бухгалтерского учета реализация информационной угрозы связана с документированием информации. Учетный документ, полученный из автоматизированной информационной системы учета, приобретает юридическую силу после того, как его подписывает должностное лицо в соответствии с законодательством Российской Федерации.

Согласно ГОСТ Р 50922-2006, существуют следующие виды информации:

– законодательная. Связана с применением законов Российской Федерации и внутренних норм организации в процессе обработки данных. Основными законами здесь являются 98-ФЗ, 149-ФЗ, 152-ФЗ, 187-ФЗ;

– физическая. Охватывает ограничение доступа к информации с использованием систем контроля доступа и физических средств блокировки;

– криптографическая. Включает методы и средства защиты информации, основанные на шифровании данных при их хранении и передаче через сеть;

– техническая. Включает в себя оборудование, устройства и программное обеспечение, такие как сканеры уязвимостей, SIEM, DLP-системы, обеспечивающие безопасность и управление информацией.

Рассмотрим основные риски безопасности учетной информации:

1. Раскрытие конфиденциальной информации.

2. Компрометация информации, получение несанкционированного доступа к сведениям и неправомерное распространение.

3. Несанкционированное использование данных.

4. Ошибки при работе в обработке информации.

5. Отказ от информации.

6. Отказ от обслуживания информации.

Также следует выделить, что современные информационные технологии в сфере бухгалтерского учета, способствуют повышению эффективности работы, но при этом несут опасность возникновения различных непредвиденных проблем, вплоть до катастрофических последствий.

Можно выделить следующие организационные способы защиты учётной информации: разработка и внедрение внутри организации правил обработки информации; проведение обучения сотрудников основам кибербезопасности и правилам работы с данным; установление областей ответственности; разработка плана восстановления данных в чрезвычайных ситуациях.

Техническими способами защиты учетной информации являются: регулярное резервное копирование критически важных данных; дублирование вспомогательных элементов информационной системы, отвечающих за хранение данных; разработка механизма экстренного перераспределения сетевых ресурсов в случае возникновения проблем или отказа отдельных компонентов; планирование использования резервных источников энергии для системы; обеспечение защиты информационных ресурсов от чрезвычайных ситуаций; использование программного обеспечения, ответственного за управление доступом к информации, осуществление мониторинга и предотвращение утечек конфиденциальных данных.

Два основных подхода к обеспечению информационной безопасности – аутентификация и идентификация, основанные на контроле доступа к информационным ресурсам. Аутентификация предполагает проверку подлинности пользователя по известным данным или идентификатору. Идентификация позволяет взаимодействовать с данными, благодаря получению уникального идентификатора пользователя в системе. При помощи этих мер регулируется управление доступом к информации и устанавливаются запреты и разрешения.

В таблице 1 приведены перечень мер для защиты учетной информации и примеры.

Таблица 1 – Меры для защиты учетной информации

№, наименование мер	Суть меры	Примеры
1. Аппаратные	Аппаратные меры безопасности представлены разнообразными электронными, электрическими и лазерными устройствами.	Генераторы кодов или электронные регистры.
2. Программные	Программные меры безопасности включают в себя программное обеспечение для ограничения доступа, проверки и блокировки трафика, а также управления сетью.	Антивирусы и брандмауэры.
3. Криптографические	Криптографические меры безопасности включают различные программы и сервисы для кодирования и шифрования информации, что предотвращает ее использование без соответствующего ключа шифрования.	Электронная подпись.
4. Физические	Физические меры безопасности включают в себя физические барьеры, которые мешают свободному доступу к данным.	Сейфы и изолированные помещения под замком.

Источник: снижение рисков безопасности данных / [Электронный ресурс] // Официальный сайт Солар: [сайт]. – URL: https://rt-solar.ru/products/solar_inrights/blog/3203/ (дата обращения: 14.04.2024).

Далее проведем анализ методов защиты учетной информации. В таблице 2 приведен перечень выделяемых методов.

Таблица 2 – Методы защиты учетной информации

№	Метод	Пример
1	Установление системы внутреннего контроля.	Контрольная среда, процесс оценки рисков, информационная система, в т. ч. связанная с подготовкой финансовой (бухгалтерской) отчетности, контрольные действия; мониторинг средств контроля.
2	Создание физических препятствий для злоумышленников.	Использование изолированных помещений, кодовых дверей и систем контроля доступа.
3	Управление информацией и регламентация работы с данными.	Разработка правил, регламентов и ограничений доступа к информации.
4	Маскировка.	Методы шифрования данных, которые делают невозможным их использование без соответствующего ключа шифрования.
5	Принуждение.	Создание условий работы с данными, исключающих возможность использования любых вариантов, кроме одного правильного, а также защита учетной информации для предотвращения угрозы материальной, административной или уголовной ответственности.
6	Стимулирование.	Создание рабочих условий, в которых сотрудников мотивируют соблюдать правила, условия и меры защиты информации при обработке данных.
7	Обучение персонала компании основам информационной безопасности.	Ознакомление с принципами работы с информацией, использование безопасных каналов передачи данных и применение стандартных и специализированных средств защиты информации.
8	Ограничение доступа к важной информации.	Наилучшим образом осуществляется через ролевую модель управления с использованием принципов минимальных привилегий.
9	Контроль над носителями	Избавление от сменных носителей, чтобы

№	Метод	Пример
	информации и источниками данных	исключить возможность кражи информации или внедрения вредоносного ПО
10	Использование шифрование данных и доверенные каналы передачи.	Зашифрованная информация затрудняет несанкционированное использование, а надежный ключ шифрования обеспечивает защиту от утечки данных.
11	Внедрение современных технологических решений для мониторинга и контроля информационных ресурсов компании	Для обеспечения полной безопасности информации можно использовать IdM/IGA, системы предотвращения утечек данных (DLP) и защитные шлюзы для контроля сетевого трафика.

Источник: способы защиты информации / [Электронный ресурс] // Официальный сайт Солар: [сайт]. – URL: URL: https://rt-solar.ru/products/solar_dozor/blog/3250/ (дата обращения: 13.04.2024).

Обеспечение безопасности учетных данных позволяет: осуществлять идентификацию и аутентификацию; регулировать возможности на выполнение действий в системе; выявлять уровень конфиденциальности документов и устанавливать индивидуальные права на просмотр; ставить электронную подпись; производить шифрование информации, совершать регистрацию действий пользователей в журналах аудита.

Так, например, при произведении поиска данных компании «Норникель» была найдена информация, указывающая на то, что идет непрерывный процесс активного развития в рассматриваемой области. «Норникель» активно развивает свою Систему управления информационной безопасностью. Эта система охватывает процессы оперативного управления производством, обеспечения сырьем и технологическими материалами, а также контроля выполнения плановых показателей по производству и отгрузке готовой продукции. Для поддержания и улучшения высокого уровня информационной безопасности «Норникель» регулярно проходит внешние аудиты, проверяющие соответствие требованиям защиты персональных данных, критической информационной инфраструктуры, а также международным

стандартам управления процессами кибербезопасности. «Норникель» на постоянной основе проводится тестирование и анализ уровня защищенности, контроль обеспечения информационной безопасности.

За последние годы в «Норникель» на Надеждинском металлургическом и Медном заводах Заполярного филиала, а также в Мурманском транспортном филиале Компании была успешно внедрена система управления информационной безопасностью в соответствии с международным стандартом ISO/IEC 27001:2013. На основании проверки внешние аудиторы отметили высокий уровень готовности «Норникеля» и соответствие международным стандартам. В Компании организован Центр реагирования на инциденты информационной безопасности, который применяет современные технологические решения и лучшие методики управления кибербезопасностью. Для предотвращения и пресечения чрезвычайных ситуаций в работе «Норникеля» разработаны процедуры и процессы обеспечения непрерывности информационной безопасности, которые периодически проверяются путем тестирования, которое проводится не реже одного раза в квартал, для повышения эффективности.

Компанией «Норникель» утвержден Регламент повышения информированности в области информационной безопасности. Для его осуществления каждый год проводятся обучающие мероприятия включающие актуальную информацию для персонала. Руководителями проводятся регулярные проверки знаний сотрудников. Для оценки работы системы, подготовки к действиям в случае угрозы информационной безопасности и повышения уровня защиты корпоративных данных проводят тренинги с имитацией фишинговых атак и других видов киберугроз. После проведения анализа результатов тренингов, пересматриваются имеющиеся и разрабатываются новые инструкции для сотрудников. Обновленная информация, полученная в результате

тренингов, включается в квартальный отчет, который распространяется среди руководителей подразделений внутри Компании.

«Норникель» и «Лаборатория Касперского» подписали соглашение о сотрудничестве. Это позволит «Норникель» повысить информационную безопасность, защитить корпоративную и промышленную инфраструктуру.

Для достижения этой цели специалисты компании будут тестировать программное обеспечение и приложения, включая сценарии использования KasperskyOS, проводить анализ безопасности, осуществлять аудит событий в области информационной безопасности с привлечением решений от «Лаборатории Касперского».

Также «Норникель» подписал соглашение о сотрудничестве с Security Vision. Цель данного партнерства заключается в укреплении защиты промышленных информационных систем и данных для обеспечения целостности и непрерывности производственных процессов в сфере металлургии. В рамках данного партнерства разрабатываются и проверяются новые решений в сфере информационной безопасности, что способствует увеличению уровня защиты от киберугроз, повышению эффективности управления рисками в области информационной безопасности и ускорению реагирования на инциденты.

По мнению представителей, крупные компании в настоящее время нуждаются в высококвалифицированных специалистах по информационной безопасности. В этой связи «Норникель» активно способствует подготовке специалистов: с 2017 года в МГИМО МИД России функционирует базовая кафедра «Корпоративная безопасность» при поддержке «Норникеля».

Заключение. Таким образом в результате данного исследования было выявлено, что ПАО «ГМК Норильский никель» показывает высокую оценку организации защиты учетной информации в условиях обеспечения

кибербезопасности, этому обуславливает сопоставление найденной информации ПАО «ГМК Норильский никель» по защите учетной информации и общая теоретическая основа защиты учетной информации, например, изучение методов информационной безопасности и возможных принятых мер для защиты учетной информации.

Использованные источники:

1. Способы защиты информации / [Электронный ресурс] // Официальный сайт Солар: [сайт]. – URL: URL: https://rt-solar.ru/products/solar_dozor/blog/3250/ (дата обращения: 13.04.2024).

2. Снижение рисков безопасности данных / [Электронный ресурс] // Официальный сайт Солар: [сайт]. – URL: https://rt-solar.ru/products/solar_inrights/blog/3203/ (дата обращения: 14.04.2024).

3. Национальный стандарт Российской Федерации защита информации основные термины и определения / [Электронный ресурс] // ГОСТ Р 50922-2006: [сайт]. – URL: https://ksc-alternativa.com.ru/wp content/uploads/2019/08/%D0%93%D0%9E%D0%A1%D0%A2-%D0%A0-50922-2006.pdf (дата обращения: 18.05.2024).

4. «Норникель» и Security Vision подписали соглашение о сотрудничестве в области информационной безопасности / [Электронный ресурс] // Норникель: [сайт]. – URL: https://nornickel.ru/news-and-media/press-releases-and-news/nornikel-i-security-vision-podpisali-soglashenie-o-sotrudnichestve-v-oblasti-informatsionnoy-bezopasnosti/ (дата обращения: 18.05.2024).

5. «Норникель» и «Лаборатория Касперского» договорились о развитии сотрудничества в области безопасности промышленной и корпоративной инфраструктуры / [Электронный ресурс] // Норникель: [сайт]. – URL:

https://nornickel.ru/news-and-media/press-releases-and-news/nornikel-i-laboratoriya-kasperskogo-dogovorilis-o-razvitii-sotrudnichestva-v-oblasti-bezopasnosti-promyshlennoy-i-korporativnoy-infrastruktury/ (дата обращения: 18.05.2024).

6. «Норникель» поделился опытом в сфере кибербезопасности / [Электронный ресурс] // Таймырский телеграф: [сайт]. — URL: https://www.ttelegraf.ru/news/nornikel-podelilsya-opytom-v-sfere-kiberbezopasnosti/ (дата обращения: 18.05.2024).