УДК 004

Рябова К.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

О НЕОБХОДИМОСТИ ПРИМЕНЕНИЯ ПРОГРАММ БЕЗОПАСНОГО ПОВЕДЕНИЯ И КУЛЬТУРЫ ИБ (SBCP)

Аннотация. В статье раскрыты особенности использования программ безопасного поведения и культуры ИБ (SBCP) на примере ПО системы мониторинга «ИНСАЙДЕР». В содержании статьи рассматриваются и анализируются проблемы обеспечения информационной безопасности в контроле и мониторинге рабочего времени сотрудников компании.

Ключевые слова: информация, система защиты информации, контроль работы, программы безопасного поведения, эффективность работы сотрудников.

В настоящее время программы безопасного поведения и культуры информационной безопасности (SBCP – Safe Behavioral Culture Programs for Information Security) являются важными инструментами для защиты организаций от инцидентов информационной безопасности (ИБ) и снижения рисков нарушения конфиденциальности, целостности и

доступности информации. Их актуальность обусловлена несколькими факторами:

1. Рост числа кибератак. Количество и сложность подобного вида атак постоянно увеличиваются с появлением новых технологий. Современные угрозы включают фишинговые атаки, программы-шифровальщики, инсайдерские риски и другие виды угроз ИБ. Для эффективной борьбы с даными рисками необходимы комплексные меры безопасности, включающие как обучение сотрудников, так и повышение уровня осведомленности о мерах предосторожности [2, с. 22].

2. Изменение законодательства. Законы и нормативные акты, регулирующие защиту персональных данных и конфиденциальной информации, становятся все строже. Например, российские законы № 152-ФЗ «О персональных данных» и № 187-ФЗ «О безопасности критической информационной инфраструктуры», а также международные стандарты, такие как GDPR (General Data Protection Regulation), требуют от компаний внедрения эффективных мер защиты информации. Программы безопасного поведения и культуры информационной безопасности помогают организациям соответствовать требованиям регуляторов и избежать штрафов и репутационных потерь.

3. Повышение ответственности сотрудников. Многие инциденты ИБ происходят из-за человеческого фактора: недостаточной внимательности, незнания правил безопасной работы с защищаемой информацией или случайных ошибок пользователей. Регулярное обучение сотрудников правилам работы с такими данными помогает снизить вероятность нарушений ИБ и повысить уровень общей защищенности информации в организации [1, с. 18–19].

Основными элементы программ SBCP являются следующие показатели: обучение и информирование: регулярные занятия, вебинары и тестирование знаний сотрудников о правилах ИБ. Разработка и внедрение инструкций и руководств по соблюдению требований информационной безопасности. Проведение мониторинга и постоянный контроль: системы мониторинга действий пользователей, проведение аудитов и проверок соблюдения политики безопасности. Управление изменениями: обеспечение постоянного обновления процедур и технологий защиты информации.

Система мониторинга «Инсайдер» является одним из примеров программ безопасного поведения и культуры информационной безопасности. Она представляет собой специализированное решение, предназначенное для выявления и предотвращения внутренних угроз информационной безопасности (инсайдеров). Она позволяет эффективно контролировать деятельность сотрудников внутри организации, предотвращая возможные утечки данных, несанкционированный доступ (НСД) к конфиденциальной информации и прочие нарушения политики безопасности.

Особенностями системы «Инсайдер» можно выделить: постоянный анализ активности пользователей. Система автоматически фиксирует и анализирует активность пользователей в сети и локальных системах организации. Это включает мониторинг операций с файлами, сетевых соединений, использование внешних устройств хранения и другие действия, потенциально угрожающие безопасности информации. Также создаются профили активности каждого сотрудника, основанные на его привычных действиях. Отклонения от нормального профиля (например, попытка скачивания большого объема данных или подключение неизвестного устройства) регистрируются системой и поступает сигнал руководству. При выявлении подозрительных действий система «Инсайдер» оперативно уведомляет службу информационной безопасности, позволяя своевременно принять необходимые меры по защите информации. Также контролируется передача файлов между сотрудниками, взаимодействие с внешними ресурсами, включая электронную почту, облачные сервисы и социальные сети [3, с. 56].

В системе «Инсайдер» имеются инструменты для быстрого анализа инцидентов информационной безопасности, сбора доказательств и составления отчетов, необходимых для дальнейшего расследования и принятия управленческих решений при возникновении угрозы. Предусмотренные в программном обеспечении автоматизированные процессы позволяют существенно сократить временные затраты на выявление потенциальных угроз и реагирование на возникающие инциденты [4, с. 48].

Стоит отметить, что преимуществами использования системы «Инсайдер» являются:

– минимизация риска утечек данных и краж интеллектуальной собственности;

– оперативное выявление потенциальных угроз ИБ, предотвращение происшествия и минимизация ущерба от инцидентов;

– улучшение эффективности службы информационной безопасности благодаря автоматизации рутинных задач и своевременному обнаружению угроз;

– повышение дисциплины и осознание важности вопросов информационной безопасности среди сотрудников.

Таким образом, использование специализированных систем, таких как «Инсайдер», становится необходимым условием устойчивого развития бизнеса и минимизации финансовых и репутационных рисков. В условиях, когда хозяйствующие субъекты постоянно сталкиваются с всевозрастающими требованиями по обеспечению информационной безопасности, особенно в условиях современных реалий и ужесточающихся нормативно-правовых актов в области защиты информации, подобные системы мониторинга значительно повышают уровень надежности организаций, предприятий, учреждений, помогая защитить их данные и бизнес-

процессы от внутренних и внешних угроз. Программы безопасного поведения и культуры информационной безопасности играют ключевую роль в обеспечении надежной защиты информации и снижении риска возникновения инцидентов ИБ в организации.

Список использованных источников:

1. Бондаренко И.С. Информационная безопасность: учебник / И.С. Бондаренко. М.: МИСИС, 2023. 254 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/360344 (дата обращения: 18.04.2025).

2. Никифорова Г.С. Психология менеджмента. Психологический практикум: учебное пособие / под ред. Г.С. Никифорова. 2-е изд. М.: Проспект, 2021. 504 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com /book/280712 (дата обращения: 18.04.2025).

3. Прохорова О.В. Информационная безопасность и защита информации: учебник для СПО / О.В. Прохорова. 6-е изд., стер. Санкт-Петербург: Лань, 2025. 124 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/445250 (дата обращения: 19.04.2025).

4. Яппаров Р.М. Роль и значение автоматизированных информационных систем в правоохранительной деятельности / Р.М. Яппаров // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов V Всероссийской молодежной научно-практической конференции, Уфа, 20–21 мая 2022 г. Уфа: Башкирский государственный университет, 2022. С. 48–53.

Ryabova K.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

ON THE NEED TO APPLY SAFE BEHAVIOR AND INFORMATION SECURITY CULTURE PROGRAMS (SBCP)

Abstract. The article reveals the features of using safe behavior and information security culture (SBCP) programs using the example of the INSIDER monitoring system software. The content of the article discusses and analyzes the problems of ensuring information security in the control and monitoring of working hours of company employees.

Keywords: information, rights, information protection, information protection system, work control, safe behavior programs, employee performance.