http://doi.org/10.35596/2522-9613-2022-28-3-65-72

*Оригинальная статья*
*Original paper*

УДК 004.056

# МЕТОДИКА СОЗДАНИЯ И СТРУКТУРА КОРПОРАТИВНОГО ПОДРАЗДЕЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В. П. КОЧИН, А. В. ШАНЦОВ

*Белорусский государственный университет (г. Минск, Республика Беларусь)*

*Поступила в редакцию 7.08.2022*



**Аннотация.** Рассмотрена проблематика обеспечения безопасности информационных ресурсов в Республике Беларусь. Определена необходимость применения и рассмотрены типы подразделений информационной безопасности для обеспечения защиты информационных ресурсов. Выделены основные принципы создания подразделения информационный безопасности корпоративного уровня. Определены задачи и основной состав корпоративного подразделения информационной безопасности, а также предложена методика расчета его структуры. Выполнен расчет нагрузки на аналитиков первого и второго уровней из состава команды корпоративного подразделения информационной безопасности. Рассчитано соотношение количества аналитиков первого и второго уровней в составе команды и определены размеры защищаемых информационных ресурсов с помощью подразделения информационной безопасности корпоративного уровня. Предложена структура корпоративного подразделения информационной безопасности и рассмотрены режимы его работы.

**Ключевые слова:** информационные технологии, информационная безопасность, подразделение информационной безопасности.

**Конфликт интересов.** Авторы заявляют об отсутствии конфликта интересов.

**Для цитирования.** Кочин В.П., Шанцов А.В. Методика создания и структура корпоративного подразделения информационной безопасности. Цифровая трансформация. 2022; 28(3): 65-72.

# METHODOLOGY OF CREATION AND STRUCTURE OF THE CORPORATE INFORMATION SECURITY UNIT

VICTOR P. KOCHIN, ARTEM V. SHANTSOV

*Belarusian State University (Minsk, Republic of Belarus)*

*Submitted 7.08.2022*



**Abstract.** The problems of ensuring the security of information resources in the Republic of Belarus are considered. The necessity of application is determined and the types of information security units to ensure the

protection of information resources are considered. The basic principles of creating a corporate-level information security unit are highlighted. The tasks and the main composition of the corporate information security unit are determined, and the methodology for calculating its structure is proposed. The load on analysts of the first and second levels from the team of the corporate information security unit was calculated. The ratio of the number of analysts of the first and second levels in the team is calculated and the sizes of the protected information resources is determined with the help of the corporate-level information security unit. The structure of the corporate information security unit is proposed and the modes of its operation are considered.

**Keywords:** information technology, information security, information security unit.

**Conflict of interests.** The authors declare no conflict of interests.

**For citation.** Kochin V.P., Shantsov A.V. Methodology of Creation and Structure of the Corporate Information Security Unit. *Digital Transformation*. 2022; 18(3): 65-72.

## Введение

В настоящее время информационные ресурсы (далее – ИР) подвергаются постоянным угрозам информационной безопасности (далее – ИБ), также возросло количество и качество кибератак на ИР Республики Беларусь. Применение даже самых совершенных архитектур защиты информации не позволяет гарантировать полную защищенность ИР [1]. Практически ежемесячно обнаруживаются новые уязвимости в программном и аппаратном обеспечении, которые могут быть проэксплуатированы злоумышленниками. Технические нормативные правовые акты по защите информации[1,2] предъявляют требования по обеспечению ИБ лишь пассивными методами. Однако для полноценной защиты ИР пассивных методов защиты недостаточно, необходимо постоянно отслеживать актуальное состояние защищенности ИР, регулярно внедрять новые методы и механизмы защиты.

Перечисленные выше факторы приводят к необходимости внедрения комплексного подхода по защите ИР [2]. Данный подход, в том числе, предполагает защиту ИР с помощью подразделений ИБ, способных обнаруживать инциденты ИБ, реагировать на них, а также проводить расследования данных инцидентов и участвовать в ликвидации их последствий. В мировой практике данные подразделения именуются как Security Operation Center (SOC), Computer Emergency Response Team (CERT) или Computer Security Incident Response Team (CSIRT).

Законодательство Республики Беларусь в ряде случаев требует от владельцев ИР иметь в своем составе подразделение, отвечающее за ИБ[3], однако цели и задачи подразделений ИБ, а также методика расчета структуры подразделений ИБ не определены.

Целью настоящей статьи являются анализ подразделения ИБ, непосредственно обеспечивающего защиту ИР корпорации (организации); определение целей и задач, а также состава подразделения ИБ; разработка методики расчета структуры подразделения ИБ.

## Основные задачи и состав подразделения ИБ

Назначение и задачи подразделений ИБ существенно отличаются в зависимости от типа подразделения ИБ. Выделяют несколько типов подразделений ИБ:

– подразделения ИБ национального уровня;

[1] О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 [Электронный ресурс]: Приказ оперативно-аналитического центра при Президенте Республики Беларусь, 20 февраля 2020 г., № 66 // Оперативно-аналитический центр при Президенте Республики Беларусь. – Режим доступа: https://oac.gov.by/public/content/files/files/law/prikaz-oac/2020%20-%2066.pdf – Дата доступа 13.01.2021.

[2] О технической и криптографической защите персональных данных [Электронный ресурс]: Приказ Оперативно-аналитического центра при Президенте Республики Беларусь, 12 ноября 2021 г., № 195 // Оперативно-аналитический центр при Президенте Республики Беларусь. – Режим доступа: https://oac.gov.by/public/content/files/files/law/prikaz-oac/2021-195.pdf. – Дата доступа 16.11.2021.

[3] О защите персональных данных [Электронный ресурс] : Закон Республики Беларусь от 7 мая 2021 г. № 99-З – Минск: Национальный правовой Интернет-портал Республики Беларусь, 2021. – 2/2819.

– иерархические (отраслевые) подразделения ИБ;

– корпоративные подразделения ИБ.

В настоящей статье анализу подвергается подразделение ИБ корпоративного уровня, непосредственно обеспечивающее защиту ИР корпорации (организации). Основной целью корпоративного подразделения ИБ (далее – подразделения ИБ) является создание и поддержание в актуальном состоянии системы защиты информации, обнаружение и противодействие атакам нарушителей на защищаемые ИР. Для эффективного обнаружения и противодействия атакам на защищаемые ИР, подразделение ИБ должно осуществлять реагирование на инциденты в масштабе времени, соответствующем масштабу времени действий нарушителя [3, с. 41]. Для соблюдения данного критерия, в одной организационной структуре подразделения ИБ должно обеспечиваться выполнение следующих задач:

– мониторинг и обработка событий в режиме реального времени;

– анализ инцидентов ИБ и реагирование на них;

– настройка и управление датчиками аналитических систем, техническое обслуживание инфраструктуры подразделения ИБ;

– разработка и внедрение инструментов подразделения ИБ.

Для решения всех перечисленных задач подразделение ИБ должно включать в себя должности:

– начальника подразделения ИБ, осуществляющего руководство работой подразделения ИБ;

– аналитика 1-го уровня, осуществляющего первичную обработку инцидентов ИБ: отсев ложных срабатываний, идентификацию инцидентов и первичное реагирование;

– аналитика 2-го уровня, осуществляющего реагирование на инциденты ИБ, переданные от аналитиков 1-го уровня;

– администратора безопасности, отвечающего за настройку правил в системах сбора и анализа событий (SIEM или SOAR);

– системного администратора (системного инженера), отвечающего за настройку инфраструктуры подразделения ИБ.

Состав подразделения ИБ может быть также дополнен специалистами по реверс-инжинирингу, кибербразведке, экспертами-криминалистами и другими специалистами – в зависимости от решаемых подразделением ИБ задач. Однако основными задачами подразделения ИБ являются: мониторинг состояния защищаемых информационных ресурсов, выявление инцидентов ИБ и реагирование на них. Данные задачи решаются с помощью аналитиков 1-го и 2-го уровней, поэтому дальнейший расчет структуры подразделения ИБ основывается на расчете нагрузки для данных специалистов.

## Расчет структуры подразделения ИБ и нагрузки на аналитика 1-го уровня

На структуру подразделений ИБ оказывают влияние требования, предъявляемые владельцами защищаемых ИР к уровню обслуживания и максимально возможному уровню затрат на процессы ИБ. Следовательно, с одной стороны подразделения ИБ должны обладать квалифицированным персоналом в области компьютерной безопасности, а с другой – подразделения ИБ должны учитывать ограничения, связанные с затратами на процессы защиты информации. Соблюдение баланса между данными требованиями, а также обеспечение эффективного функционирования подразделения ИБ достигается его оптимальной организационной структурой.

Аналитик 1-го уровня выполняет задачи по обнаружению инцидента, его идентификации и осуществляет первичное реагирование на выявленный инцидент. Задачи аналитика 1-го уровня условно подразделяются на две части: выявление инцидента или отсев ложных срабатываний и первичное реагирование на выявленный инцидент. Расчет максимальной нагрузки на аналитика 1-го уровня основывается на возможностях по выявлению инцидентов ИБ. Время на выявление инцидента определяется по формуле:

$$T_{\text{выявл}} = T_{\text{обн}} + T_{\text{идент}}, \quad (1)$$

где $T_{\text{обн}}$ – время, необходимое на обнаружение аномальных событий, $T_{\text{идент}}$ – время, требуемое для идентификации инцидента.

Время выявления инцидента ИБ может варьироваться в широких пределах, так как оно зависит от уровня подготовленности аналитика 1-го уровня, нагрузки на него, количества анализируемых событий и сложности инцидента ИБ. В дальнейшем, для оценки максимальной возможности аналитика 1-го уровня по выявлению инцидентов, примем минимальное время обнаружения инцидента и минимальное время идентификации инцидента равными 1 минуте. Тогда, согласно формуле (1), минимально необходимое время на обнаружение инцидента ИБ составит 2 минуты. Исходя из минимально возможного времени выявления инцидента ИБ следует, что максимальные возможности аналитика 1-го уровня по выявлению инцидентов приблизительно составляют 30 инцидентов в час.

Для дальнейшего анализа будет использоваться максимально возможное значение 30 выявленных инцидентов в час. Исходя из данного значения оценим максимальное количество устройств в защищаемых ИР, которые способен отслеживать один аналитик 1-го уровня по формуле:

$$K_{\max} \geq \left( \sum_{i=1}^{N} N_i \frac{S_i}{24} \right) \cdot M , \quad (2)$$

где $K_{\max}$ – максимальное количество обнаруживаемых инцидентов в час, $N_i$ – количество отслеживаемых устройств (узлов), $S_i$ – количество событий, генерируемое устройством $N_i$ за одни сутки; $M$ – коэффициент, учитывающий частоту возникновения событий ИБ.

Частота возникновения событий (коэффициент $M$) зависит от ИР: как часто они подвергается атакам, какая политика безопасности применяется; поэтому значение коэффициента $M$ может варьироваться в широком диапазоне от 1 срабатывания на 100 событий до 1 срабатывания на 10 000 событий.

Значение $S_i$ определяется на каждом из устройств защищаемых ИР политикой безопасности. При данной настройке необходимо соблюсти баланс:

– чрезмерный сбор событий приводит к потере полезного сигнала в «шумах» и существенной нагрузке на системы сбора и анализа событий;

– недостаточный сбор событий приводит к неспособности осуществить корректную оценку события.

Рассмотрим подразделение ИБ, в котором не используются средства автоматизации. Отсутствие средств автоматизации сбора событий не позволяет осуществлять анализ широкого спектра событий – следовательно, значение среднего количества событий, генерируемых одним устройством, будет минимально необходимым и составит $S_i = 100$ [3, с. 193], а коэффициент частоты возникновения событий ИБ примет свое максимально возможное значение $M = 1/100$. Применив формулу (2), получим: $N \leq 720$. Таким образом, без средств автоматизации возможности аналитика 1-го уровня будут ограничены не более чем 720 устройствами. Под устройствами (узлами) понимаются как отдельные физические устройства – маршрутизаторы, межсетевые экраны, сервера и др., так и виртуальные устройства – виртуальные машины, контейнеры и пр.

Показатель 720 устройств (узлов) – это теоретически максимально возможный показатель для непрерывного режима работы. На практике этот показатель окажется значительно меньше: например, если подразделение ИБ работает не в круглосуточном режиме, данное значение уменьшится более чем в 3 раза и составит приблизительно 200 устройств (узлов). Для повышения производительности необходимо использовать средства автоматизации, способные представлять аналитику 1-го уровня уже обработанные события, а также способные самостоятельно проводить корреляцию событий и выявлять инциденты. Наиболее производительными решениями в данной области являются системы SIEM.

Эффективность систем SIEM обуславливается способностью в автоматическом режиме отслеживать подозрительные события и проводить корреляцию между ними. Таким образом аналитику выдается сообщения лишь об подозрительных событиях, требующих его внимания. Системы SIEM позволяют увеличить среднее количество отслеживаемых событий на устройствах до $S_i = 500$, а также значительно снижают количество ложных инцидентов до значения «одно срабатывание на 10 000 событий» ($M = 1/10\,000$) [4].

Используя формулу (2), максимально возможное количество отслеживаемых устройств (узлов) аналитиком 1-го уровня составит $N_{\max} = 14\,400$.

На практике, максимально значение отслеживаемых устройств (узлов) будет значительно меньше. Дополнительно, с увеличение масштабов ИР, увеличивается сложность физической и логической архитектуры. Исходя из указанного выше, максимально возможное количество отслеживаемых устройств (узлов) аналитиком 1-го уровня с помощью систем SIEM будет находиться в диапазоне 2000–5000 устройств (узлов).

### Масштаб защищаемых информационных ресурсов

Еще одним фактором, влияющим на структуру подразделения ИБ, являются размеры ИР клиента. Как уже было отмечено, небольшие размеры информационных ресурсов клиентов экономически не позволят содержать подготовленную команду специалистов подразделения ИБ, а также не позволят инвестировать в продвинутые системы сбора и анализа событий и другие инструменты подразделения ИБ. С другой стороны, слишком большие размеры защищаемых ИР приведут к тому, что подразделение ИБ окажется неспособным реагировать на инцидент в масштабе времени нарушителя. Нижняя граница размеров защищаемых ИР определяется экономической целесообразностью содержания подразделения ИБ и составляет приблизительно 2000–5000 устройств (узлов). Данное значение коррелирует с усредненным максимальным показателем количества узлов, которые способен отслеживать один аналитик 1-го уровня с помощью SIEM систем. Этот факт обуславливается важностью внедрения в подразделение ИБ продвинутых систем автоматизации сбора событий. Справедливость данного утверждения подтверждается оценкой соотношения значений максимального числа устройств, отслеживаемых аналитиком 1-го уровня с помощью SIEM систем и без средств автоматизации $\frac{N_{\max}}{N} = \frac{14\,400}{720} = 20$.

Следовательно, внедрение SIEM системы позволяет существенно повысить эффективность работы аналитиков 1-го уровня и является приоритетной задачей при создании подразделения ИБ. Таким образом, нижняя граница размеров защищаемых ИР (от 2000 устройств (узлов)) позволит внедрить в подразделении ИБ продвинутые системы автоматизации и сбора событий, и позволит содержать команду квалифицированных аналитиков 1-го уровня.

Максимальные размеры защищаемых ИР одним подразделением ИБ, как и количество аналитиков 1-го уровня, имеют свой предел. Расчет значения верхней границы защищаемых информационных ресурсов выходит за рамки настоящей статьи, так как на данное значение не оказывает влияние количество аналитиков 1-го и 2-го уровней.

### Режим работы подразделения ИБ и расчет нагрузки на аналитика 2-го уровня

Подразделение ИБ в большинстве случаев работает в режимах работы 8/5 или 24/7, т. е. восьмичасовой рабочий день пять дней в неделю или непрерывный круглосуточный режим работы. В Республике Беларусь установлена 40 часовая рабочая неделя[4]. Следовательно, при режиме работы 8/5 рабочая нагрузка составляет 40 часов в неделю, что соответствует требованиям законодательства. При работе подразделения ИБ в режиме 24/7 рабочая нагрузка составляет 168 часов в неделю, что потребует пятикратного увеличения числа сотрудников подразделения ИБ.

На необходимое количество аналитиков 2-го уровня оказывают влияние размеры защищаемого ИР и режим работы подразделения ИБ. Зависимость от размеров защищаемых ИР носит косвенный характер. Количество аналитиков 2-го уровня напрямую зависит от количества аналитиков 1-го уровня, чье количество, в свою очередь, зависит от размеров защищаемых ИР. Размеры защищаемых ИР не влияют на соотношение числа аналитиков 1-го и 2-го уровней, а определяют их общее необходимое количество. Режим работы подразделения ИБ, напротив, оказывает непосредственное влияние на необходимое количество аналитиков 2-го уровня и определяет соотношение между числом аналитиков 1-го и 2-го уровней.

[4] Трудовой кодекс Республики Беларусь [Электронный ресурс] : 26 июля 1999 г. № 296-З : Принят Палатой представителей 8 июня 1999 года : Одобрен Советом Республики 30 июня 1999 года // ЭТАЛОН. Действующие кодексы Республики Беларусь. – Минск, 2022.

При работе подразделения ИБ в режиме 8/5 нагрузка на аналитика 2-го уровня будет выше всего. Связано это с тем, что в начале рабочего дня, особенного первого рабочего дня недели, аналитики 2-го уровня будут задействованы вместе с аналитиками 1-го уровня в анализе событий за нерабочий период. А в случаях обнаружения инцидентов за нерабочий период, аналитики 2-го уровня должны будут сразу осуществлять реагирования на них, без первичной обработки аналитиками 1-го уровня. При работе подразделения ИБ в режиме 24/7 существует два варианта работы аналитиков 2-го уровня: работа в режиме 24/7 или работа в режиме 8/5. Минимальная нагрузка на аналитика 2-го уровня достигается при совместной круглосуточной работе аналитиков 2-го и 1-го уровней. Это обусловлено тем, что аналитик 2-го уровня может незамедлительно начать реагирование на инциденты ИБ в требуемых случаях. При режиме работы аналитика 2-го уровня 8/5, в начале рабочей недели нагрузка может быть выше из-за инцидентов, выявленных в нерабочее время. На соотношение аналитиков 1-го и 2-го уровней также влияют квалификация аналитиков 1-го уровня, количество инцидентов, передаваемых с 1-го уровня на 2-й, сложность переданных инцидентов и частота возникновения инцидентов. Данные факторы имеют субъективный характер и не позволяют формализовать расчет соотношения аналитиков 1-го и 2-го уровней. В зарубежной литературе [5] приводятся значения соотношений аналитик 2-го уровня / аналитик 1-го уровня от 1:5 до 2:1. Исходя из выполненного анализа и практики применения подразделений ИБ[5], соотношения аналитик 1-го уровня / аналитик 2-го уровня примут значения, представленные в табл. 1.

**Таблица 1**. Соотношения аналитик 1-го / 2-го уровня для различных режимов работы подразделений ИБ

**Table 1.** Ratios of 1st/2nd level analysts for various modes of operation of information security units

| Режим работы<br>Operating mode | Соотношение аналитиков 1-го / 2-го уровня<br>The ratio of 1st / 2nd level analysts |
|---|---|
| 8/5 для аналитиков 1-го и 2-го уровней | 1 аналитик 2-го уровня на 2 аналитика 1-го уровня (1:2) |
| 24/7 для аналитиков 1-го уровня и 8/5 для аналитиков 2-го уровня | 1 аналитик 2-го уровня на 3 аналитика 1-го уровня (1:3) |
| 24/7 для аналитиков 1-го и 2-го уровней | 1 аналитик 1-го уровня на 3–4 аналитика 1-го уровня (от 1:3 до 1:4) |

Описание действий команды подразделения ИБ по обнаружению инцидентов выходит за рамки настоящей статьи.

Кратко рассмотрим задачи, решаемые аналитиками 1-го и 2-го уровней. Аналитик 1-го уровня осуществляет мониторинг защищенности ИР с помощью средств автоматизации сбора событий, в частности SIEM систем. В задачи мониторинга входят: анализ событий, обнаружение инцидентов, отсев ложных срабатываний и идентификация обнаруженных инцидентов ИБ. После обнаружения инцидента ИБ, аналитик 1-го уровня действует по заранее подготовленному шаблону действий исходя из идентифицированного инцидента ИБ. Это может быть блокировка IP-адреса, изоляция машины, удаление вредоносного вложения в почтовых сообщениях, помещение файлов в карантин, восстановление системы из резервной копии и др. В случаях, когда аналитик 1-го уровня не способен самостоятельно осуществить реагирование на инцидент ИБ или не может точно идентифицировать инцидент ИБ, то инцидент передается аналитику 2-го уровня.

Аналитик 2-го уровня получает от аналитика 1-го уровня данные о выявленном инциденте и о принятых первичных мерах. Аналитик 2-го уровня не опирается на заранее подготовленные шаблоны реагирования, а анализирует ситуацию, сопоставляя обнаруженные события и факты.

[5]West-Brown M. J., D. Stikvoort, Kossakowski K.-P., Killcrece G., Ruefle R., Zajicekm M. “Handbook for Computer Security Incident Response Teams (CSIRTs)” [Electronic resourse]. – Access mode: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305. – Date of access: 13.02.2014

Аналитик 2-го уровня не ограничен по времени реагирования на выявленный инцидент и может использовать экспертную поддержку экспертов-криминалистов и специалистов по реверс-инжинирингу. Аналитик 2-го уровня также осуществляет проверку корректности действий аналитиков 1-го уровня: правильность идентификации инцидентов, отнесения инцидентов ИБ к ложным срабатываниям или принятия ложных срабатываний за инцидент ИБ.

## Заключение

В настоящей статье предложена методика расчета структуры подразделения ИБ, обеспечивающего защиту корпоративных ИР; определены цели и задачи, а также состав корпоративного подразделения ИБ.

Основой команды подразделения ИБ является группа, состоящая из аналитиков 1-го и 2-го уровней. Минимальный размер данной группы составляет 3 человека в соотношении 1:2. Максимальный размер группы – 5 человек в соотношении 1:4. Увеличение размеров защищаемых информационных ресурсов приводит к увеличению числа таких групп в составе подразделения ИБ. Помимо групп из аналитиков, в состав подразделения ИБ входят администратор безопасности, системный администратор (системный инженер) и начальник подразделения ИБ. Количество администраторов безопасности и системных администраторов зависит от размеров защищаемых информационных ресурсов и, как правило, их количество не превышает 1–2 специалистов.

Таким образом, минимальный размер команды подразделения ИБ составит 6 человек для защиты ИР с размерами в 2000–5000 устройств (узлов). Увеличение размеров защищаемых информационных ресурсов приводит к увеличению числа групп аналитиков в составе подразделения ИБ. На размер команды подразделения ИБ оказывает влияние и режим работы: так, при непрерывном круглосуточном режиме работы максимальный размер команды может составить порядка 50–60 человек.

Защиту ИР с размерами менее 200 устройств (узлов) целесообразно возложить на системных администраторов. При размерах ИР от 200 до 2000 устройств (узлов) обязанности по защите ИР необходимо осуществлять с помощью нескольких широкопрофильных специалистов в области ИБ.

## Список литературы


1. Кочин, В. П. Проблемы проектирования комплексной системы защиты информации облачных ресурсов в Республике Беларусь / В. П. Кочин, А. В. Шанцов // Цифровая трансформация. – 2021. – № 3. – С. 34– 39.
2. Кочин, В. П. Комплексная система защиты информации облачных ресурсов. / В. П. Кочин, А. В. Шанцов // Комплексная защита информации: материалы XXVI научно-практической конференции, Минск, 25–27 мая 2021 г. – С. 332–334.
3. Zimmerman, C. Ten strategies of a world-class cybersecurity operations center / C. Zimmerman. – Bedford: MITRE, 2014.
4. Bejtlich, R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response / R. Bejtlich. – San Francisco: No StarchPress, 2013.
5. Bejtlich, R. The TAO of Network Security Monitoring: Beyond Intrusion Detection / R. Bejtlich. – San Francisco, No StarchPress, 2013.


## References


1. Kochyn, V.P. Problems of designing complex information security system for cloud resources in the Republic of Belarus / V. P. Kochyn, A. V. Shantsou // Cifrovaja transformacija [Digital transformation]. – 2021. – Vol. 3 (16). – P. 34–39. (In Russ.)
2. Kochyn, V.P. Integrated system of information protection of cloud resources / V. P. Kochyn, A. V. Shantsou // Kompleksnaya zashchita informacii: Materialy XXVI nauchno-prakticheskoj konferencii Kompleksnaya zashchita informacii. [Comprehensive information protection: Materials of the XXVI scientific-practical conference Comprehensive information protection]. – Minsk, 2021. – P. 332–334. (In Russ.)
3. Zimmerman, C. Ten strategies of a world-class cybersecurity operations center / C.Zimmerman. – Bedford: MITRE, 2014.

4. Bejtlich, R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response / R. Bejtlich. – San Francisco: No StarchPress, 2013.
5. Bejtlich, R. The TAO of Network Security Monitoring: Beyond Intrusion Detection / R. Bejtlich. – San Francisco, No StarchPress, 2013.

## Вклад авторов

Авторы внесли равный вклад в написание статьи.

## Authors contribution

The authors made an equal contribution to the writing of the article.

**Сведения об авторах**

**Кочин В. П.,** к. т. н., начальник центра информационных технологий Белорусского государственного университета.

**Шанцов А. В.,** аспирант кафедры технологий программирования Белорусского государственного университета.

**Адрес для корреспонденции**

220030, Республика Беларусь, г. Минск,
пр-т Независимости, 4,
Белорусский государственный университет;
+375 29 842-23-14;
e-mail: downseason@mail.ru
Шанцов Артем Владимирович

**Information about the authors**

**Kochin V. P.,** Cand. Of Sci.., Head of the Information Technology Center of the Belarusian State University.

**Shantsou A. V.,** Cand. Of Sci., Postgraduate at the Department of Programming Technologies of the Belarusian State University.

**Address for correspondence**

220030, Republic of Belarus, Minsk,
Nezavisimosti Ave., 4,
Belarusian State University;
+375 29 842-23-14
e-mail: downseason@mail.ru
Shantsou Artem Vladimirovich