УДК 004.056

СТРУКТУРА И СОСТАВ КОРПОРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.П. Кочин[1], А.В. Шанцов[2]

[1]Белорусский государственный университет,
пр-т Независимости, 4, 220030, г. Минск, Беларусь, Kochyn@bsu.by
[2]Белорусский государственный университет,
пр-т Независимости, 4, 220030, г. Минск, Беларусь, ShantsovAV@bsu.by

Рассмотрена проблематика обеспечения безопасности информационных ресурсов в Республики Беларусь. Определена необходимость применения подразделений информационной безопасности для обеспечения защиты информационных ресурсов. Рассмотрены типы подразделений информационной безопасности. Определены цели и задачи корпоративного подразделения информационной безопасности. Рассмотрены требования к инфраструктуре и средствам автоматизации подразделения информационной безопасности корпоративного уровня. Определен основной состав корпоративного подразделения информационной безопасности. Предложены структуры корпоративных подразделений информационной безопасности. Приведены краткие характеристики подразделений информационной безопасности корпоративного уровня в зависимости от масштабов защищаемых информационных ресурсов.

Ключевые слова: информационные технологии; информационная безопасность; подразделение информационной безопасности.

STRUCTURE AND COMPOSITION OF CORPORATE INFORMATION SECURITY UNITS

V.P. Kochyn[a], A.V. Shantsou[b]

[a]Belarusian State University, 4 Niezalieznasci Avenue, Minsk 220030, Belarus,
Kochyn@bsu.by
[b]Belarusian State University, 4 Niezalieznasci Avenue, Minsk 220030, Belarus,
ShantsovAV@bsu.by

The problems of ensuring the security of information resources in the Republic of Belarus are considered. The necessity of using information security units to ensure the protection of information resources is determined. The types of information security units are considered. The goals and objectives of the corporate information security unit are defined. The requirements for the infrastructure and automation tools of the corporate-level information security unit are considered. The main composition of the corporate information security unit has been determined. The structures of corporate information security unit are proposed. Brief characteristics of corporate-level information security units are given depending on the scale of protected information resources.

Keywords: information technology; information security; information security unit.

Введение

В настоящее время информационные ресурсы (далее – ИР) подвергаются постоянным угрозам информационной безопасности (далее – ИБ). Применение хорошо продуманных архитектур защиты информации не позволяет гарантировать полную защищенность ИР [1]. Новые уязвимости в программном и аппаратном обеспечении, позволяют злоумышленникам разрабатывать новые методы преодоления средств защиты. На сегодняшний день в Республике Беларусь технические нормативные правовые акты по защите информации предъявляют требования по обеспечению ИБ лишь пассивными методами [2,3]. Однако, для полноценной защиты ИР пассивных методов защиты недостаточно, необходимо постоянно отслеживать актуальное состояние защищенности ИР, регулярно внедрять новые методы и механизмы защиты.

Вышеперечисленные факторы приводят к необходимости внедрения комплексного подхода по защите ИР [4]. Данный подход в том числе предполагает защиту ИР с помощью подразделений ИБ, способных обнаруживать инциденты ИБ, реагировать на них, проводить расследования данных инцидентов, участвовать в ликвидации их последствий, проводит постоянный мониторинг событий ИБ, внедрять новые методы и механизмы защиты информации. В мировой практике, в зависимости от решаемых задач и масштабов защищаемых информационных ресурсов, данные подразделения именуется как Security Operation Center (SOC), Computer Emergency Response Team (CERT) или Computer Security Incident Response Team (CSIRT). Назначение и задачи подразделений ИБ существенно отличаются в зависимости от типа подразделения ИБ. Выделяют несколько типов подразделений ИБ:

подразделения ИБ национального уровня;

иерархические (отраслевые) подразделения ИБ;

корпоративные подразделения ИБ.

Актуальность проблемы защиты ИР с помощью подразделений ИБ обусловлено также тем, что законодательство Республики Беларусь в ряде случаев требует от владельцев ИР иметь в своем составе подразделение, отвечающее за ИБ [5], однако цели и задачи подразделений ИБ, а также методика расчета структуры подразделений ИБ не определены.

Методология исследования

В настоящей статье анализу подвергается подразделение ИБ корпоративного уровня, непосредственно обеспечивающее защиту ИР корпора-

ции (организации) (далее – подразделение ИБ). Анализ основывается на теоретических основах по защите информации, методикам противодействия кибератакам, а также лучшим мировым практикам по созданию подразделений ИБ.

Цели и задачи подразделения ИБ

Целью подразделения ИБ является обеспечение информационной безопасности защищаемых ИР. Для достижения данной цели, подразделение ИБ решает задачи в зависимости от структуры и масштабов защищаемых ИР, а также необходимого уровня защиты ИР. Основными задачами, решаемыми подразделением ИБ, являются:

инвентаризация защищаемых активов и поддержание информации о них в актуальном состоянии;

мониторинг и обработка событий и сетевого трафика в режиме реального времени;

анализ действий пользователей;

анализ уязвимостей и контроль их устранения;

поведенческий анализ файлов;

проверка устойчивости информационных ресурсов к внешним воздействиям (тесты на проникновение);

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

обработка информации об инцидентах ИБ, проведение расследований инцидентов ИБ, анализ инцидентов ИБ и реагирование на них;

проведение тренировок по реагированию на инциденты ИБ;

разработка и внедрение инструментов подразделения ИБ.

Подразделение ИБ, в зависимости от защищаемых ИР и требований по их защите, решает либо часть из перечисленных задач, либо решает задачи в полном объеме, а также в отдельных случаях решает дополнительные задачи для поддержания требуемого уровня защиты ИР.

Для решения поставленных задач, подразделения ИБ должно включать: инфраструктуру, средства автоматизации и персонал.

Инфраструктура и средства автоматизации подразделения ИБ

При функционировании подразделения ИБ немаловажную роль играет инфраструктура. Необходимо предусмотреть масштабирование инфраструктуры подразделения ИБ для наращивания объемов хранения информации, усиления отказоустойчивости при сборе событий ИБ и

увеличения скорости обработки данных. Обязательным является подготовка инфраструктуры к хранению больших объемов данных.

К средствам автоматизации подразделений ИБ относят такие системы, как система сбора и анализа информации о событиях информационной безопасности SIEM (Security Information and Event Management), система оркестрировки, автоматизации и реагирования SOAR (Security Orchestration Automation and Response), система сбора событий LM (Log Management). Применение систем SIEM и SOAR является приоритетной задачей, так как позволяет существенно сократить затраты на человеческие ресурсы по сравнению с другими средствами автоматизации.

Дополнительно в подразделении ИБ используются такие средства автоматизации, как средства реверс-инжиниринга, средства сбора криминалистических доказательств, сетевые сканеры, сканеры уязвимостей и другие. Применение средств автоматизации в составе подразделения ИБ позволяет существенно снизить штат подразделения ИБ, что в свою очередь позволяет инвестировать в подготовку персонала вместо найма большего количества. Модель подразделения ИБ с меньшим числом подготовленных специалистов имеет экономические преимущества по сравнению с моделью с большим числом сотрудников среднего уровня подготовленности [6].

Персонал подразделения ИБ

В независимости от структуры подразделения ИБ, для эффективного противодействия атакам на защищаемые ИР, подразделение ИБ должно осуществлять реагирование на инциденты ИБ в масштабе времени, соответствующим масштабу времени действий нарушителя [7, 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.

Для решения перечисленных задач в составе подразделения ИБ должны быть:

- Руководитель подразделения ИБ. Руководитель подразделения ИБ осуществляет общее руководство работой подразделения ИБ, координирует взаимодействие между командой подразделения ИБ. Осуществляет подбор кадров, управление финансами подразделения ИБ, проводит работу с потенциальными и существующими клиентами.

- Аналитик 1-го уровня. Аналитик 1-го уровня осуществляет первичную обработку инцидентов ИБ – распределение и первичный отсев ложных срабатываний. Аналитики 1-го уровня в работе опираются на заранее созданные администратором безопасности сценарии реагирования, в которых указана последовательность шагов, которые надо предпринять при обнаружении того или иного типа инцидента ИБ. В случае, если аналитик 1-го уровня может самостоятельно выполнить все действия, он осуществляет реагирование своими силами. Если он столкнулся с необходимостью эскалации инцидента ИБ, то он передает его на следующий уровень – аналитику 2-го уровня. На аналитиков 1-го уровня также возлагается взаимодействие с клиентами (прием заявок, звонков).
- Аналитик 2-го уровня. Аналитик 2-го уровня получает данные об инцидентах от аналитика 1-го уровня. Аналитик 2-го уровня не опирается на какие-либо шаблоны реагирования, а анализирует уникальную ситуацию, сопоставляя различные события и факты, имеющие отношение к инциденту ИБ. В случае, если в расследуемой кибератаке применялось ранее неизвестное вредоносное ПО или применен новый тип атаки, аналитик 2-го уровня, при реагировании на инцидент ИБ, взаимодействует с реверс-инженерами и экспертами-криминалистами (при их наличии в составе подразделения ИБ).
- Администратор безопасности. Администратор безопасности отвечает за настройку правил в системах SIEM (SOAR). Администратор безопасности получает исходные данные о работе информационных систем и составляет правила выявления инцидентов и реагирования на них. Это правила корреляции в системах SIEM, которые отвечают за обработку входящих сообщений от систем безопасности и за выстраивание этих разнородных событий в логически целостную «историю» для поиска возможной атаки, а также правила автоматического реагирования, локализации, восстановления информационных систем при помощи SOAR решений. Совместно с аналитиками 2-го уровня осуществляет написания сценариев реагирования для аналитиков 1-го уровня. В случае, если для защиты используются системы обнаружения/предотвращения вторжений, то на администратора безопасности возлагаются функции по написанию для них сигнатур.
- Системный администратор (системный инженер) – лицо ответственное за настройку и поддержание работоспособности инфраструктуры подразделения ИБ. В обязанности системного администратора входит конфигурирование различных типов операционных систем, прикладного программного обеспечения, систем

защиты, сетевого оборудования. В случае, если в подразделении ИБ используется какое-то самостоятельно созданное программное обеспечение (далее – ПО), то на системного администратора (системного инженера) возлагают функции непрерывной интеграции и настройки такого ПО (функции DevOps).

Наличие указанных должностей в составе подразделения ИБ является обязательным. Важно отметить, что выше приведены именно должности, а не состав подразделения ИБ. Для повышения уровня защищенности ИР и повышения уровня обслуживания в составе подразделения ИБ дополнительно предусматриваются следующие должности:

- Специалист по реверс-инжинирингу (реверс-инженер). Реверс-инженер выполняет задачи по изучению образцов вредоносного ПО для противодействия осуществляемым с их помощью кибератакам. При выявлении нового вредоносного ПО, на реверс-инженера возлагаются функции по написанию сигнатур вредоносного ПО.
- Эксперт-криминалист. На эксперта-криминалиста возлагаются задачи по поиску изменений (аномалий) в атакованной системе, определение данных, которые были удалены, изменены или похищены, определение систем, которые были атакованы. На эксперта-криминалиста возлагаются задачи по воссозданию полного пути распространения атаки: что именно подвергалось атаке, как развивалась атака и какой был причинен ущерб.
- Специалист по кибербразведке. Специалист по кибербразведке отвечает за поиск уязвимостей в защищаемых ИР, по согласованию с владельцами ИР выполняет тестирование на проникновение. Дополнительно специалист по кибербразведке осуществляет аудит защищаемых ИР с целью обнаружения вредоносных программ в системах, например вирусов-логических бомб, которые срабатывают только при наступлении определенных условий, а до этого никак себя не проявляют. На данного специалиста возлагают функции по поиску информации о новых типах атак и уязвимостей.

Рассмотренный перечень должностей команды подразделения ИБ позволяет решать все задачи, возлагаемые на подразделение ИБ. В определенных случаях обязанности каждого из членов команды могут дополняться в зависимости от решаемых задач.

Структура подразделения ИБ

Подразделение ИБ может быть как независимой организацией, оказывающей услуги в форме аутсорсинга, так и структурно входить в состав

компании, ИР которой подлежат защите. В отдельных случаях, подразделение ИБ не будет выделяться как таковое, вместо этого задачи по защите ИР будут возложены на системных администраторов ИР. На структуру подразделения ИБ оказывает влияние необходимый уровень обслуживания (защиты) ИР и допустимый уровень затрат на защиту ИР.

Для эффективного функционирования и соблюдения требований клиентов, структура подразделения ИБ должна соответствовать трем критериям [7, с. 49]:

1. Подразделение ИБ должно обладать квалифицированным персоналом в области защиты информации.
2. Подразделение ИБ, в частности инфраструктура, должна обеспечивать максимальную эффективность при сборе и обработке событий ИБ, анализе циркулирующего трафика в ИР.
3. Подразделение ИБ должно учитывать экономические ограничения клиентов по защите ИР и ограничения полномочий подразделения ИБ при предотвращении атак на ИР.

Выбор верной структуры подразделения ИБ позволяет соблюсти баланс между вышеперечисленными критериями и обеспечить максимальную эффективность функционирования подразделения ИБ. Рассмотрим варианты структур подразделений ИБ в зависимости от масштабов защищаемых ИР.

Нижняя граница защищаемых ИР структурно-независимым подразделением ИБ составляет порядка 2000 – 5000 устройств (узлов). Данное подразделение ИБ является либо независимой организацией, либо структурным подразделением компании-владельца ИР. Для решения задач по защите ИР указанных масштабов подразделение ИБ должно обладать собственной инфраструктурой, средствами автоматизации (SIEM или SOAR). Следовательно, в составе подразделения ИБ будет администратор безопасности и системный администратор.

Масштаб защищаемых информационных ресурсов до 10 000 узлов, позволит эффективно функционировать, с экономической точки зрения, только в режиме 8/5 (5 дней в неделю по 8 часов). При этом, для обеспечения защиты ИР масштабов от 2 000 до 10 000 устройств (узлов), потребуется две группы из аналитиков 1-го и 2-го уровней в соотношении два аналитика 1-го уровня на одного аналитика 2-го уровня.

Предлагаемая структура подразделения ИБ представлена на рисунке 1.

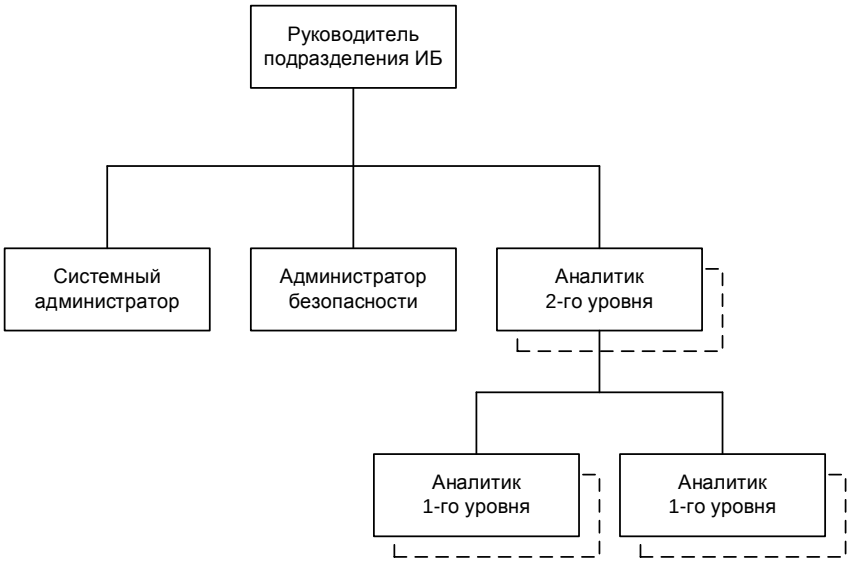

Рисунок 1 – Структура подразделения ИБ

Увеличение масштабов защищаемых ИР или необходимость в предоставлении более высокого уровня обслуживания при защите ИР приводят к необходимости расширения подразделения ИБ, а также к необходимости перехода к круглосуточному режиму работы подразделения ИБ (части подразделения ИБ).

Как правило ИР с масштабами более 10 000 устройств (узлов) не являются однородными и состоят из множества информационных систем (далее – ИС). Для повышения эффективности защиты ИС проводятся тестирования на проникновение, выявляющие слабые места в системе защиты ИС. За каждой ИС закрепляется группа из аналитиков 1-го и 2-го уровней, обладающих максимальной осведомленностью о составе и структуре, защищаемой ИС. Также, высокий уровень защищенности ИР подразумевает наличие в составе подразделения ИБ реверс-инженера и эксперта-криминалиста. Основными задачами данных специалистов является экспертная поддержка аналитиков 2-го уровня при расследовании сложных инцидентов ИБ.

Увеличение масштабов защищаемых ИР приводит к увеличению масштабов инфраструктуры подразделения ИБ, количества датчиков аналитическим систем и числа собираемых событий ИБ. Следовательно, увеличиться и количество администраторов безопасности и системных администраторов.

Круглосуточный режим работы подразделения ИБ подразумевает круглосуточную работу аналитиков 1-го уровня. При этом режим работы аналитиков 2-го уровня варьируется: 8/5 или 24/7. На практике, из-за отсутствия необходимости в столь высоком уровне обслуживания и эконо-

мической целесообразности, чаще используется режим работы аналитиков 2-го уровня 8/5. Таким образом, будут применяться группы из аналитиков 1-го и 2-го уровней в соотношении три аналитика 1-го уровня на одного аналитика 2-го уровня. При этом, под аналитиками 1-го уровня подразумевается рабочее место, так как при режиме работы 24/7 на одно рабочее место будет приходится 4 – 5 сотрудников. Количество групп аналитиков 1-го и 2-го уровней зависит от масштабов защищаемых информационных ресурсов и может варьироваться в пределах от 2 до 4 групп. В предлагаемой структуре подразделения ИБ выделено 3 таких группы.

Предлагаемая структура расширенного подразделения ИБ приведена на рисунке 2.

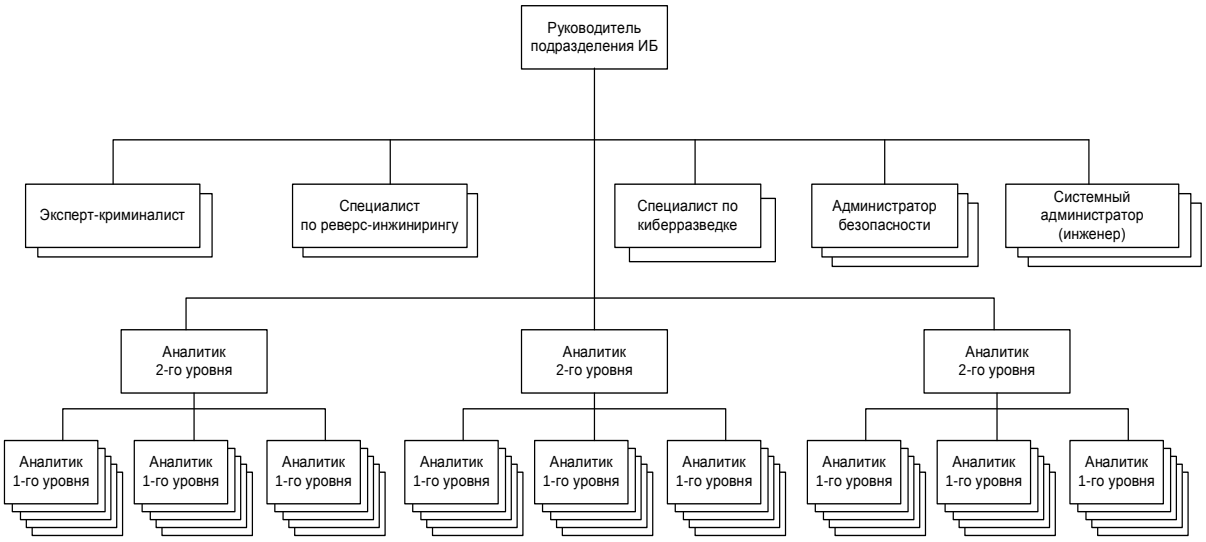

Рисунок 2 – Структура расширенного подразделения ИБ

При размерах защищаемых ИР менее 2 000 устройств (узлов) защита с использованием полноценного подразделения ИБ является экономически нецелесообразной. Для обеспечения защиты ИР данных масштабов применяют «виртуальное» подразделение ИБ. Термин «виртуальное» подразумевает, что подразделение ИБ не имеет необходимой команды в полном составе, либо команда подразделения ИБ частично состоит из специалистов совмещающих выполнение обязанностей нескольких должностей, в том числе и за пределами подразделения ИБ.

«Виртуальное» подразделение ИБ использует инфраструктуру ИР, следовательно, отсутствует необходимость в системном администраторе. Если настройка средств защиты осуществляется системными администраторами ИР, то также отсутствует необходимость в администраторе безо-

пасности. В данном случае «виртуальное» подразделение ИБ будет состоять лишь из аналитиков 1-го и 2-го уровней, при этом на аналитика 2-го уровня возлагаются задачи по руководству командой. Предлагаемая структура «виртуального» подразделения ИБ представлена на рисунке 3.

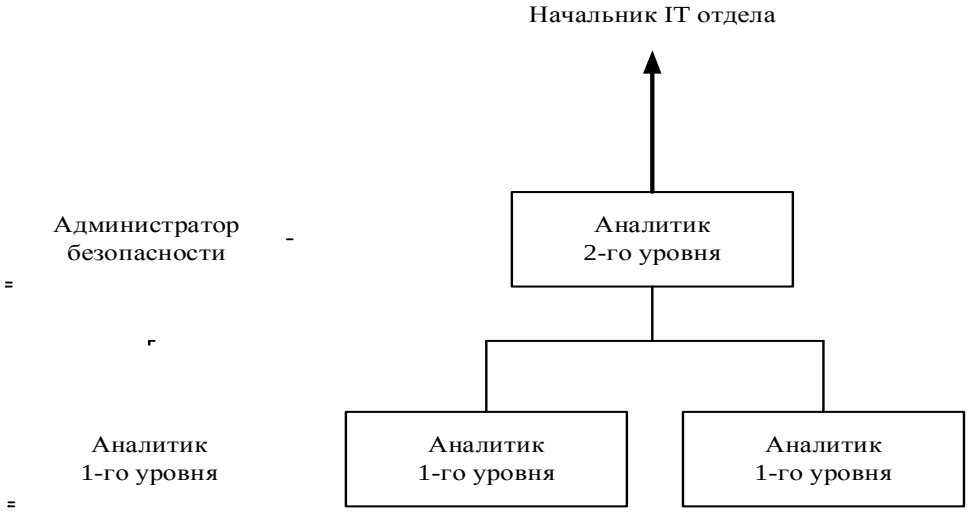

Рисунок 3 – Структура «виртуального» подразделения ИБ

При защите ИР с размерами порядка 500 устройств (узлов), применение подразделений ИБ является нецелесообразным. Данные масштабы ИР позволяют системным администраторам ИР самостоятельно поддерживать необходимый уровень защищенности. При этом необходимо, чтобы из команды системных администраторов было назначено лицо, непосредственно отвечающее за защиту ИР.

Обобщенная характеристика подразделений ИБ в зависимости от масштабов защищаемых ИР приведена в таблице.

Таблица – Характеристики подразделений ИБ

Подразделение ИБ	Ориентировочные размеры защищаемых ИР	Краткая характеристика
Защита системными администраторами ИР	До 500	Обеспечение защиты ИР командой системных администраторов; назначение из состава системных администраторов ответственного лица за защиту ИР.
«Виртуальное» подразделение ИБ	500 – 3 000	Отсутствие или совмещение ряда должностей в составе подразделения ИБ; отсутствие собственной инфраструктуры, использование инфраструктуры защищаемых ИР; отсутствие аналитических систем (SIEM, SOAR); отсутствие полномочий по самостоятельному

		реагированию на выявленные инциденты ИБ; входит в состав компании владельца информационных ресурсов.
Подразделение ИБ	3 000 – 10 000	Наличие собственной инфраструктуры; применение аналитических систем сбора и анализа событий (SIEM, SOAR); совместное реагирование на инциденты вместе с владельцами ИР; функционирование в режиме 8/5; входит в состав компании владельца ИР или является самостоятельной организацией.
Расширенное подразделение ИБ	От 10 000	Наличие собственной инфраструктуры; применяются системы автоматизации сбора и анализа событий, инструменты киберкриминалистики, реверс-инжиниринга и другие, в том числе самостоятельно разработанные; обладает полномочиями по самостоятельному реагированию на инциденты ИБ; частично функционирует в режиме 24/7; обслуживает крупные компании, информационные ресурсы которых часто подвергаются атакам и требуют высокого уровня защиты.

Заключение

В настоящем анализе определен состав и предложены структуры подразделений ИБ. Рассмотрена зависимость структуры подразделения ИБ от масштабов защищаемых ИР, необходимого уровня обслуживания и максимально возможного уровня затрат. Предложены структуры подразделений ИБ в зависимости от масштабов защищаемых ИР и решаемых задач.

Приведенные границы масштабов ИР для выбора типа подразделения ИБ не являются точными и носят рекомендательный характер. Например, ИР государственных учреждений, ИР, обрабатывающие персональные данные, априори требуют более высокий уровень защиты независимо от их масштабов. При определении того или иного типа подразделения ИБ, владельцы ИР должны определить, что для них является более приоритетным: высокий уровень защищенности при высоком уровне затрат, или достаточный уровень защищенности при среднем уровне затрат.

Активная защита информации с помощью подразделений ИБ играет важную роль при защите ИР. Непрерывное совершенствование методов проведения атак на ИР, создание и развитие новых средств для проведения кибератак делают уязвимыми пассивные системы защиты информа-

ции. Для обеспечения комплексности, система защиты информации должна состоять как из пассивной, так и из активной составляющих. Таким образом, активная защита с помощью подразделений ИБ является неотъемлемой частью комплексной системы защиты информации.

Библиографические ссылки

1. Кочин В.П., Шанцов А.В., Проблемы проектирования комплексной системы защиты информации облачных ресурсов в Республике Беларусь // Цифровая трансформация. 2021; № 3. С. 34–39.
2. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449». Минск: Оперативно-аналитический центр при Президенте Республики Беларусь, 2021.
3. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195 «О технической и криптографической защите персональных данных». Минск: Оперативно-аналитический центр при Президенте Республики Беларусь, 2021.
4. Кочин В.П., Шанцов А.В., Комплексная система защиты информации облачных ресурсов // Материалы XXVI научно-практической конференции «Комплексная защита информации». НП РУП «Научно-исследовательский институт технической защиты информации». 2021. С. 332 – 334.
5. Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных». Минск: Национальный правовой Интернет-портал Республики Беларусь, 2021.
6. Rajnovic D. Computer Incident Response and Product Security. Indianapolis: Cisco Press, 2011.
7. Zimmerman C. Ten strategies of a world-class cybersecurity operations center. Bedford: MITRE, 2014.