Добро должно быть с кулаками,
Добро суровым быть должно,
Чтобы летела шерсть клоками
Со всех, кто лезет на добро…

Станислав Кунаев

Киберучения на киберполигоне

как эффективный инструмент поиска уязвимостей

Олег БОСЕНКО,
директор департамента кибербезопасности IBS

Что есть противостояние добра и зла в информационном пространстве? Добро – это всегда мы. А зло – все то, что мешает нашим информационным процессам или хочет вообще прекратить их. Значит, надо быть готовыми к противодействию злу. Однако без понимания существа зла, опыта и навыков борьбы такая готовность немного стоит. Как же прийти к такому пониманию? Что дают киберучения и киберполигоны? Можно ли с их помощью получить ценный опыт и навыки? Ответам на эти вопросы и будет посвящена статья.

Киберучения и киберполигон: целевое предназначение

Для начала стоит ответить на три вопроса: зачем нужны киберучения, зачем нужны киберполигоны, являются ли киберучения и киберполигоны неразрывно связанными элементами.

В нормативно-правовых документах мы не найдем определения понятия «киберучения». В информационной поддержке кибербезопасности присутствуют лишь понятийные определения, которые в общем случае можно свести к следующему: киберучения (англ. Adversary Emulation) – это процесс формирования и отработки навыков по выявлению компьютерных атак и/или реагированию на инциденты информационной безопасности у специалистов подразделений информационной безопасности и смежных подразделений, а также отработка методик использования инструментов защиты (методик применения СОИБ[1]). Кроме того, целью учений может быть проверка информационных объектов, информационных систем и их совокупностей на возможность противостоять кибератакам. Следовательно, киберучения – один из элементов подготовки СУИБ[2] к возможным кибератакам, а также комплексная проверка правильности настроек и алгоритмов функционирования СОИБ для отражения/блокирования кибератак.

Киберучения строятся на замысле проведения, который формируется на основе предполагаемых сценариев кибератак. Исходя из замысла разрабатывается план проведения киберучений и необходимые информационные и технологические документы для проведения.

Киберучения могут быть трех видов:

- **штабные** – отрабатываются порядок действий подразделений и их взаимодействие при отражении кибератак. При этом порядок действий может отрабатываться совместно с профильными и контролирующими подразделениями регуляторов;
- **технологические** – проверяется правильность настроек и алгоритмов применения СОИБ для отражения/блокирования кибератак. Технологические киберучения включают в себя и отработку порядка действий подразделений;
- **комплексные** – отрабатываются и порядок действий, и технологические аспекты безопасности.

[1] *СОИБ – система обеспечения информационной безопасности.*
[2] *СУИБ – система управления информационной безопасностью.*

Киберучения могут быть односторонними и двусторонними. Общая классификация киберучений приведена на схеме.

Следует отметить, что штабные киберучения являются односторонними – отрабатывается только защита. Действия атакующей стороны закладываются либо в исходную обстановку, либо в наращивание обстановки.

Технологические киберучения могут быть односторонними (анализируется эффективность защиты) и двусторонними (анализируется эффективность защиты при рандомном изменении кибератак). Примером двусторонних киберучений можно считать проводимый на регулярной основе Standoff.

Комплексные киберучения всегда двусторонние, в ходе их анализируются эффективность защиты и действия обучаемых. Они могут проводиться с заранее подготовленным подыгрышем обстановки или с рандомно проводимыми кибератаками, когда играющим на «темной стороне» предоставляется свобода выбора вариантов атаки.

Здесь есть важный момент. Проводить технологические и комплексные киберучения на реальной ИТ-инфраструктуре и системе защиты организации или отрасли – это риск снижения эффективности защиты при ошибке в формировании замысла, риск срыва процессов. В этом случае и используется киберполигон как база для проведения киберучений.

В отличие от «киберучений» термин «киберполигон» имеет в Российской Федерации правовое закрепление. Постановление Правительства РФ от 12 октября 2019 г. № 1320 «Об утверждении Правил предоставления субсидий из федерального бюджета на введение в эксплуатацию и обеспечение функционирования киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности» дает

Рис. 1. *Схема. Классификация киберучений по видам*

четкое определение: «Киберполигон» – инфраструктура для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них».

Основным элементом в определении является то, что инфраструктура киберполигона – это самостоятельный информационный объект, не связанный с общей ИТ-инфраструктурой. По существу, киберполигон представляет собой технологическую площадку имитации ИТ- и ИБ-инфраструктуры, а также деструктивных действий для отработки киберучений, тренировок и тестирования. Для эффективности киберучений площадка киберполигона должна обеспечивать высокую степень имитации. Чем имитация ближе к реальности, тем более высокий эффект дадут проводимые на киберполигоне мероприятия.

Преимущества задействования киберполигона для симуляции атак на информационные объекты очевидны. Смоделировав ИТ- и ИБ-инфраструктуру, ИТ- и ИБ-подразделения на практике проверяют, могут ли они заблаговременно обнаружить воздействие на инфраструктуру либо целевую атаку до того, как она дойдет до финальной стадии, релевантны ли разработанные на этот случай регламенты, налажено ли взаимодействие между ИТ и ИБ, а также между другими подразделениями.

> Киберполигон можно считать обязательным элементом комплексных и технологических киберучений.

Таким образом, киберполигон можно считать обязательным элементом комплексных и технологических киберучений. Киберучения, в свою очередь, представляют собой организационно-технические мероприятия, нацеленные на выработку решений по совершенствованию системы информационной безопасности.

Стоит отметить, что возможности киберполигонов не ограничиваются киберучениями. Это еще и образовательная площадка для специалистов по кибербезопасности, с помощью которой можно отработать порядок действий в формате учебы. Примером является использование «Национального киберполигона» для обучения и переподготовки специалистов Ростелекома.

Поиск уязвимостей и «узких» мест в ходе киберучений

Если говорить о перечне задач, которые могут быть решены и решаются в ходе киберучений, то в качестве основных можно выделить следующие:

- отработка совместных действий подразделений по детектированию и отражению кибератак;
- взаимодействие с государственными системами противодействия компьютерным угрозам и соответствующими подразделениями регулятора;
- поиск «узких» мест в СОИБ и их устранение или минимизация рисков;
- обучение сотрудников подразделений безопасности действиям в критичных ситуациях;
- формирование эффективных решений по функционированию СОИБ и СУИБ в критичных ситуациях.

Остановимся на поиске уязвимых мест и для начала ответим на вопрос, все ли уязвимые места можно определить в ходе киберучений.

Таблица 1. Методы выявления «узких» мест

«Узкие» места	Методы выявления
Недостаточная функциональность технических средств защиты информации	Количественная и качественная оценки детектируемых в динамике атак
Отсутствие или несовершенство алгоритмов действий СУИБ при кибератаках или в иных критических ситуациях	Уточнение перечня и содержания организационных и организационно-технических процессов противодействия атакам
Недостаточный профессионализм сотрудников подразделений безопасности	Формирование сложной оперативной обстановки в ходе учений и оценка действий обучаемых
Недостаточное ресурсное обеспечение информационной безопасности для противодействия кибератакам	Анализ ресурсного обеспечения для противодействия комплексным атакам
Психологическая неустойчивость сотрудников подразделений безопасности в критических ситуациях	Проигрыш стресс-сценариев в ходе учений

К уязвимым местам СОИБ и СУИБ относятся:

- недостаточная функциональность технических средств защиты информации;
- наличие уязвимостей в программном обеспечении информационных систем, телекоммуникационного оборудования и средств защиты информации;
- отсутствие или несовершенство алгоритмов действий СУИБ при кибератаках или в иных критичных ситуациях;
- недостаточное ресурсное обеспечение информационной безопасности для противодействия кибератакам;
- недостаточный профессионализм сотрудников подразделений безопасности;
- психологическая неустойчивость сотрудников подразделений безопасности в критичных ситуациях.

Есть некоторые сложности со сканированием ПО на уязвимости, поскольку это вопрос рутинный и его отработка в ходе учений не является необходимостью. Если же это заложено в план киберучений, то, скорее всего, организаторы не совсем понимают суть мероприятия.

Что касается остальных «узких» мест, то их выявление должно быть положено в планирующие документы киберучений. При этом следует обратить внимание на методы выявления слабых мест (табл. 1).

Для отработки всех перечисленных задач необходим киберполигон как место проведения киберучений.

> Возможности киберполигонов не ограничиваются киберучениями. Это еще и образовательная площадка для специалистов по кибербезопасности

Методы моделирования и методики проведения киберучений

Более подробно рассмотрим планирование киберучений, применяемые методы моделирования и методики проведения.

Планирующие документы для проведения киберучений должны включать:

- замысел проведения киберучений;
- расчет привлекаемых организационных и технических ресурсов;
- план проведения киберучений;
- план наращивания обстановки перед началом и в ходе проведения киберучений;
- перечень допущений обстановки;

- методику оценки успешности/неуспешности действий;
- методику подведения итогов киберучений.

Кому-то может показаться, что этот перечень напоминает военную тематику проведения учений. Противостояние в информационной сфере действительно близко к военному: есть нападающая сторона, есть обороняющаяся, есть способы нападения (кибератаки) и способы защиты (СОИБ и СУИБ).

В зависимости от вида киберучений перечень документов может различаться. Состав документов по видам приведен в табл. 2.

Качественное проведение киберучений в большой степени зависит от грамотного моделирования направленности, структуры и динамики возможного деструктивного воздействия. Важно сформировать перечень отрабатываемых угроз, количество и динамику кибератак, представить картину комбинированных атак и изменения векторов атак. Умение сделать это можно отнести к категории искусства. Все вышеизложенное должно найти отражение в замысле киберучений. Для его разработки целесообразно привлечь специалистов не только ИБ, но и ИТ-, и бизнес-подразделений.

В основу моделирования для подготовки замысла стоит заложить следующие документы:
- анализ текущей ситуации с атаками и инцидентами;
- методический документ ФСТЭК «Методика оценки угроз безопасности информации»;
- методический документ ФСТЭК «Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Если киберучения проводятся на уровне федерального округа, субъекта Федерации, отрасли либо крупной компании с госучастием, лучше согласовать замысел киберучений со специализированными подразделениями ФСТЭК и ФСБ России. В условиях массовой цифровизации, обострения геополитической обстановки и санкций наблюдается рост количества кибератак. При этом злоумышленники становятся изобретательнее, ставят перед собой более амбициозные цели, совершенствуют тактики и техники своих действий.

Таблица 2. Состав планирующих документов по видам киберучений

Планирующие документы	Виды киберучений		
	Штабные	Технологические	Комплексные
Замысел проведения киберучений	Да	Да	Да
Расчет привлекаемых организационных и технических ресурсов	Нет	Да	Да
План проведения киберучений	Да	Да	Да
План наращивания обстановки перед началом и в ходе проведения киберучений	Да	Да	Да
Перечень допущений обстановки	Да	Нет	Нет
Методика оценки успешности/неуспешности действий	Да	Нет	Да
Методика подведения итогов киберучений	Да	Да	Да

Сложности интерпретации результатов и выработки рекомендаций

Нарастает применение технологий искусственного интеллекта для кибератак. Это значит, что необходимы более тщательная проверка в ходе киберучений и правильная оценка полученных результатов.

Зачастую результатом киберучений является доклад об их успешном проведении, решении всех планируемых задач и получении подтверждения готовности системы защиты информации к отражению кибератак. Все довольны, все хорошо, ведь получен результат, который ждут «наверху». Но действительно важным является формирование перечня результатов киберучений, полученных по завершении. В общем случае это будут аналитические и прогнозные материалы, подтверждающие либо опровергающие эффективность СОИБ.

Результаты киберучений могут быть сведены в три группы:
- первая – результаты оценки эффективности СОИБ по отражению нарастающих кибератак;
- вторая – результаты оценки эффективности СУИБ при управлении и отражении кибератак;
- третья – результаты оценки подготовленности сотрудников подразделений безопасности к действиям по отражению кибератак.

По каждой группе формируется перечень конкретных и измеряемых результатов. В нынешних условиях следует стремиться опираться на измеряемые результаты и в меньшей степени – на качественные оценки.

Таким образом, на современном уровне развития и реализации информационной безопасности киберучения являются самой эффективной формой комплексной отработки управленческих и организационно-технических решений, позволяющей подготовить подразделения информационной безопасности и смежные подразделения к противостоянию в информационно-телекоммуникационном пространстве. ■